LINEA NETWORK
PROFESSIONAL

Wireless N 150Mbps ADSL2+ Router

Manuale

WebShare Torrent 242 WN

ITALIANO

Questo prodotto è coperto da garanzia Atlantis **Fast-Swap** della durata di 2 anni. Per maggiori dettagli in merito o per accedere alla documentazione completa in Italiano fare riferimento al sito **www.atlantis-land.com.**

ENGLISH

This product is covered by Atlantis 2 years **Fast-Swap** warranty. For more detailed informations please refer to the web site **www.atlantis-land.com.**
For more detailed instructions on configuring and using the Switch, please refer to the online manual.

FRANCAIS

Ce produit est couvert par une garantie Atlantis **Fast-Swap** de 2 ans. Pour des informations plus détaillées, référez-vous svp au site Web **www.atlantis-land.com.**

DEUTSCH

Dieses Produkt ist durch die Atlantis 2 Jahre **Fast-Swap** Garantie gedeckt. Für weitere Informationen, beziehen Sie sich bitte auf Web Site **www.atlantis-land.com.**

ESPAÑOL

Este producto està cubierto de garantía Atlantis **Fast-Swap** por 2 años. Para una información más detallada, se refiera por favor al Web site **www.atlantis-land.com.**

INDICE

A.5 Interfaccia WLAN 126

A02-RAU242-WN(v1.0)_MI01 (v1.00 Dicembre 2010)

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

Restrizioni di responsabilità CE/EMC

Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.

Se il prodotto fosse utilizzato con un PC/apparati non certificati, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l'utilizzatore è responsabile della "compliance" con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.

CE Mark Warning

In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

Dichiarazione di Conformità

Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo

riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-1, EN 301 489-17(compatibilità elettromagnetica) ed EN 60950(sicurezza). Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:

Francia(FR): Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per informazioni ulteriori consultare *www.art-telecom.fr.*

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestichi genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.

Italia(IT): Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: *www.comunicazioni.it.*

Lussemburgo: Se utilizzato per servizi network o privati è da richiedere l'autorizzazione.
Norvegia (NO): apparecchiatura da non utilizzare in un aresa geografica di 20 km di raggio nei pressi di Ny Alesund.
Russia (CCP): solo per uso interno.

Dichiarazione di Conformità Sintetica

Con la presente dichiariamo che questo apparato è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttive 1999/5/CE. La dichiarazione di conformità nella sua forma completa è disponibile presso il sito www.atlantis-land.com (alla pagina del prodotto) o può essere richiesta a info@atlantis-land.com.

Importanti informazioni per il corretto riciclaggio/smaltimento di questa apparecchiatura

Il simbolo qui sotto indicato, riportato sull'apparecchiatura elettronica da Lei acquistata e/o sulla sua confezione, indica che questa apparecchiatura elettronica non potrà essere smaltita come un rifiuto qualunque ma dovrà essere oggetto di raccolta separata.
Infatti i rifiuti di apparecchiatura elettroniche ed elettroniche devono essere sottoposti ad uno specifico trattamento, indispensabile per evitare la dispersione degli inquinanti contenuti all''interno delle apparecchiature stesse, a tutela dell'ambiente e della salute umana. Inoltre sarà possibile riutilizzare/riciclare parte dei materiali di cui i rifiuti di apparecchiature elettriche ed elettroniche sono composti, riducendo così l'utilizzo di risorse naturali nonché la quantità di rifiuti da smaltire.
Atlantis, in qualità di produttore di questa apparecchiatura, è impegnato nel finanziamento e nella gestione di attività di trattamento e recupero dei rifiuti di apparecchiature elettriche ed elettroniche compatibili con l'ambiente e con la salute umana.
E' Sua responsabilità, come utilizzatore di questa apparecchiatura elettronica, provvedere al conferimento della stessa al centro di raccolta di rifiuti di apparecchiature elettriche ed elettroniche predisposto dal Suo Comune. Per maggiori informazioni sul centro di raccolta a Lei più vicino, La invitiamo a contattare i competenti uffici del Suo Comune.
Qualora invece avesse deciso di acquistare una nuova apparecchiata elettronica di tipo equivalente e destinata a svolgere le stesse funzioni di quella da smaltire, potrà portare la vecchia apparecchiatura al distributore presso cui acquista la nuova. Il distributore sarà tenuto ritirare gratuitamente la vecchia apparecchiatura[1].
Si tenga presente che l'abbandono ed il deposito incontrollato di rifiuti sono puniti con sanzione amministrativa pecuniaria da € 103 a € 619, salvo che il fatto costituisca più grave reato. Se l'abbandono riguarda rifiuti non pericolosi od ingombranti si applica la sanzione amministrativa pecuniaria da € 25 a € 154.

Il suo contributo nella raccolta differenziata dei rifiuti di apparecchiature elettriche ed elettroniche è essenziale per il raggiungimento di tutela della salute umana connessi al corretto smaltimento e recupero delle apparecchiature stesse.

1 Il distributore non sarà tenuto a ritirare l'apparecchiatura elettronica qualora vi sia un rischio di contaminazione del personale incaricati o qualora risulti evidente che l'apparecchiatura in questione non contiene i suoi componenti essenziali o contiene rifiuti diversi da apparecchiature elettriche e/o elettroniche.

NB: le informazioni sopra riportate sono redatte in conformità alla Direttiva 2002/96/CE ed al D. Lgs. 22 luglio 2005, n.[·] che prevedono l'obbligatorietà di un sistema di raccolta differenziata nonché particolari modalità di trattamento e smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE). Per ulteriori informazioni in materia, la invitiamo a consultare il nostro sito www.atlantis-land.com

AVVERTENZE

- Utilizzare esclusivamente l'antenna fornita a corredo. Antenne diverse e/o con guadagno differente potrebbero violare le normative vigenti. Atlantis si intende sollevata da ogni responsabilità in caso di utilizzo di accessori (antenne e/o alimentatori) non contenuti nell'imballo.
- Lasciare almeno 30cm di distanza tra l'antenna del dispositivo e l'utilizzatore.
- Non usare il dispositivo in un luogo in cui ci siano condizioni di alte temperatura ed umidità, il dispositivo potrebbe funzionare in maniera impropria e danneggiarsi.
- Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del dispositivo in oggetto
- Non aprire mai il case del dispositivo né cercare di ripararlo da soli.
- Se il dispositivo dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.
- Non appoggiare il dispositivo su superfici plastiche o in legno che potrebbero non favorire lo smaltimento termico.
- Mettere il dispositivo su una superficie piana e stabile
- Usare esclusivamente l'alimentatore fornito nella confezione, l'uso di altri alimentatori farà automaticamente decadere la garanzia.
- Non effettuare upgrade del firmare utilizzando apparati/client wireless ma solo wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.
- I settaggi Wireless di default consentono un funzionamento ottimale del dispositivo, si invita a non cambiare il campo **TX Power Level.**

	Tutte le condizioni di utilizzo, avvertenze e clausole contenute in questo manuale e nella garanzia si intendono note ed accettate. Si prega di restituire immediatamente (entro 7 giorni dall'acquisto) il prodotto qualora queste non siano accettate.

La marcatura CE con il simbolo di attention Mark (CE ⓘ) poste sull'etichetta di prodotto potrebbero non rispettare le dimensioni minime stabilite dalla normativa a causa delle ridotte dimensioni di quest'ultima.

Atlantis invita a visitare il sito web www.atlantis-land.com alla relativa pagina di prodotto per reperire manualistica e contenuti tecnici (aggiornamenti driver e/o funzionalità, utility, support note) aggiornati.

Il logo WEEE ( ) posto sull'etichetta di prodotto potrebbe non rispettare le dimensioni minime stabilite dalla normativa a causa delle ridotte dimensioni di quest'ultima.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT o a consumo. Atlantis non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. **In caso di dubbio contattare preventivamente l'assistenza tecnica.**

Per usufruire delle condizioni di garanzia migliorative associate al prodotto (Fast Swap, On Site e On Center) è opportuno provvedere alla registrazione dello stesso sul sito www.atlantis-land.com entro e non oltre 15 giorni dalla data di acquisto. La mancata registrazione entro il termine di sopra farà si che il prodotto sia coperto esclusivamente dalla condizioni standard di garanzia.

La ringraziamo per aver scelto un router della famiglia WebShare, la via più semplice per il Wireless networking. Questa manuale fornisce tutti i dettagli sull'uso del prodotto.

1. PANORAMICA DI PRODOTTO

Condivisione dell'Accesso ad Internet e dell'IP

WebShare 242 WN dispone di 4 porte Fast Ethernet (con auto negoziazione 10/100Mbps) per la connessione alla Lan e consente, grazie al modem ADSL2+ integrato, un downstream sino a 24Mbps. Dotato di funzionalità NAT permette a diversi utenti di navigare in Internet e condividere simultaneamente la connessione ADSL usando un solo abbonamento con l'ISP ed un singolo indirizzo IP.

Wireless N 150Mbps

Grazie all'Access Point integrato, basato sulle più recenti specifiche 802.11n (sino a 150Mbps), è possibile realizzare reti wireless ad alte performance. L'antenna rimuovibile da 5 dBi assicura inoltre la completa eliminazione delle zone morte. La funzionalità WDS permette, connettendo sino a 4 Access Point, di estendere la copertura wireless anche in zone remote.

Firewall e Qualità del Servizio (QoS)

Il Router dispone di un sofisticato firewall integrato che include funzionalità avanzate di ispezione dei pacchetti, DoS ed URL Filtering. Il dispositivo ha la capacità di istradare con priorità prestabilite pacchetti in funzione della loro precedenza (IP e tipo di servizio). Sono proposte differenti classi di servizio. La velocità di navigazione non verrà più rallentata a causa dei programmi P2P utilizzati su altri computer.

BitTorrent™, Print Server USB e 3G USB Modem

Il client BitTorrent™ integrato permette il download di contenuti (che verranno salvati sul dispositivo di archiviazione connesso alla porta USB) da Internet anche a PC spento, consentendo così un importante risparmio energetico. Grazie al server FTP integrato è possibile accedere ai file memorizzati sia da postazione locale che da Internet. Alternativamente, sempre tramite la porta USB, è possibile la condivisione di una stampante che diviene a tutti gli effetti una stampante di rete. Infine è possibile collegare alla porta USB 2.0 un modem 3G/HDSPA utilizzabile sia come connessione primaria (laddove il servizio ADSL non è disponibile) che configurato in modalità Main Connection Backup in modo da garantire connettività sempre attiva alla rete anche nel caso di fail-over della linea ADSL.

Fa**cile da usare e configurare**

Tramite la comoda interfaccia Web è possibile accedere velocemente e facilmente a tutte le funzioni offerte dal Router. Il dispositivo può essere configurato anche da remoto via Web, indipendentemente dal tipo di abbonamento ADSL, grazie alla funzione Dynamic DNS integrata.

	WebShare 242 WN è stato progettato per essere conforme alle normative vigenti nelle nazioni appartenenti alla Comunità Europea e anche a quelle in vigore negli stati extra CE. L'utente dovrà pertanto utilizzare il dispositivo senza mai cambiare il campo **TX Power Level (Advanced->Basic Setting->Wireless)** dal valore di default. Atlantis S.p.a. si solleva da qualsiasi responsabilità derivante da eventuali modifiche o utilizzo improprio del prodotto. Per maggiori dettagli consultare il manuale online alla pagina del prodotto.

1.1 Requisiti di sistema

Prima di procedere con l'installazione del prodotto verificare di disporre dei seguenti requisiti:

- Protocollo TCP/IP installato in ogni PC
- Un browser WEB quali Internet Explorer 5.0 o superiore, Netscape Navigator 6.0 o superiore

1.2 CONTENUTO DELLA CONFEZIONE

Prima dell'utilizzo, verificare che la scatola contenga i seguenti elementi:

- Router WebShare Torrent 242WN
- Una guida rapida in Italiano, Inglese e francese
- Alimentatore AC-DC (9V@1,5A)
- Cavo di rete CAT-5, Cavo RJ11 e Antenna da 5 dBi
- Cd-Rom contenente manualistica multilingua e driver
- Coupon di Garanzia e WEEE

Nel caso in cui il contenuto non sia quello sovradescritto, contattare il proprio rivenditore immediatamente.

1.3 I LED frontali

LED	SIGNIFICATO
STATUS	Lampeggiante (1 volta al secondo) in verde durante il corretto funzionamento. Acceso verde fisso quando dispositivo di storage è connesso. Lampeggiante (più volta al secondo) in verde durante situazioni anomale o quando il dispositivo è in recovery mode.
WAN	Spento quando la linea ADSL non viene rilevata. Acceso verdo quando sincronizzato con il DSLAM (condizione necessaria alla navigazione). Lampeggiante in caso di trasmissione/ricezione dati.
WLAN	Accesso verde quando il modulo wireless è operativo. Lampeggiante in caso di trasmissione/ricezione dati.
1-4	Acceso verde in caso di collegamento a 100/10 Mbps. Lampeggiante in caso di trasmissione/ricezione dati.
Reset	Dopo che il dispositivo è acceso, effettuare per effettuare il reset la seguente procedura: Premere **Wireless ON/OFF** e **WPS** per circa 5 secondi. Il LED Status si spegnerà, per indicare l'avvenuto reset dell'apparato.
ON/OFF	Pulsante per accensione spegnimento.

1.4 Le porte posteriori

PORTA	SIGNIFICATO
PWR	Connettere l'alimentatore fornito a corredo a questo jack. Quando l'alimentatore va collegato al dispositivo il bottone di accensione dovrebbe essere su OFF.
USB	Connettere alla porta USB la stampante, dispositivo di archiviazione o modem 3G.
Ethernet (1-4)	Connettere con un cavo UTP.
DSL (RJ11)	Connettere il cavo RJ11 a questa porta per effettuare l'allacciamento all'ADSL.
R-SMA	Avvitare delicatamente l'antenna da 5 dBi fornita.

1.5 Settaggi di Default

Prima di iniziare la configurazione del WebShare Torrent 242 WN è necessario conoscere i settaggi di default. Utilizzando questi settaggi e impostando i PC come client DHCP (come da istruzioni seguenti) ed infine configurando la connessione all'ISP (tutti i parametri della connessiona ADSL devono essere noti) è possibile utilizzare il dispositivo in pochissimo tempo. Per una configurazione dettagliata fare riferimento al manuale presente sul CD. Le configurazioni di Default sono:

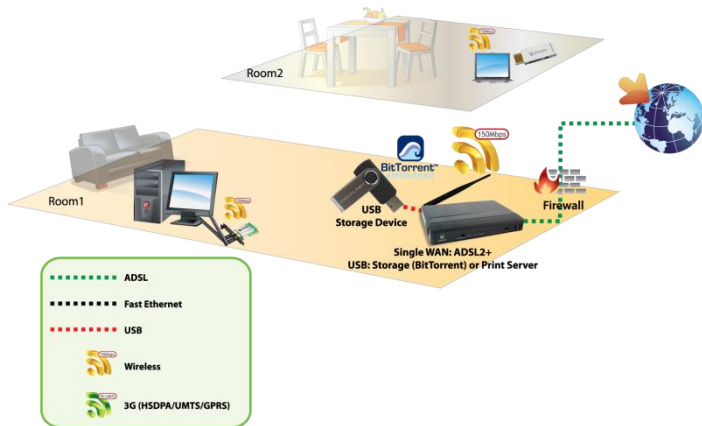
- Username: **admin**
- Password: **atlantis**
- LAN IP Address: **192.168.1.254**

- Subnet Mask: **255.255.255.0**
- WAN: **PPPoA, VCMux, Routing, VPI=8, VCI=35**
- SSID: **A02-RAU242-WN**, Sicurezza: **WPA2-PSK (AES)**
- Chiave WPA precondivisa: **WebShare242WN**
- **DHCP Server abilitato** (IP pool da **192.168.1.100** a 192.168.1.199)

1.6 Cablaggio

Anzitutto collegare il prodotto alla linea **ADSL** tramite il cavo RJ11 fornito in dotazione (nella porta DSL), poi collegare alle porte RJ45 i PC della Lan oppure eventuali Switch. E' possibile accedere al Router tramite un client Wireless o tramite il cavo di rete. Infine collegare l'alimentatore al Wireless Router ADSL2+ e poi alla presa elettrica. Una volta controllati tutti i collegamenti ed acceso il Wireless Router ADSL2+ il prodotto effettuerà immediatamente una diagnostica (circa 60 secondi).
I Led frontali supporteranno l'utenza in una fase di diagnostica preliminare; lo stato degli stessi, al termine del processo di boot, dovrà essere come indicato di seguito:

LED	Stato
STATUS	Acceso verde fisso o lampeggiante
LAN 1-4	Acceso verde/arancio lampeggiante nel caso di dispositivi collegati
WLAN	Acceso verde lampeggiante/fissa
WAN	Acceso verde fisso

Il Led WAN diventerà fisso, una volta allineatosi (condizione indispensabile per la navigazione Internet).
Poiché l'ADSL ed il normale servizio telefonico condividono (spesso) lo stesso filo per trasportare i rispettivi segnali è necessario, al fine di evitare interferenze dannose, dividere tramite un apposito filtro i 2 segnali. Tale filtro passa basso permetterà di estrarre la porzione di spettro utilizzata dal servizio telefonico impedendo così che la qualità di questo sia compromessa dalle alte frequenze introdotte dal segnale dell'ADSL. E' necessario pertanto utilizzare un filtro per ogni presa su cui è collegato un telefono analogico. Atlantis consiglia i modelli A01-AF1 o A01-AF2. In figura un tipico esempio di installazione.

1.7 Configurazione di IE

Al fine di permettere la navigazione Internet tramite il WebShare, di seguito riportiamo la configurazione necessaria per i più comuni browser presenti sul mercato:

Internet Explorer 7/8

- Cliccare col tasto destro del mouse sull'icona e selezionare la voce **Proprietà**.
- Selezionare la scheda Connessioni e spuntare l'opzione **Non utilizzare mai connessioni remote**.

Mozilla Firefox 3.0

- Avviare il browser Mozilla Firefox
- Cliccare sulla **Strumenti** - >**Opzioni**
- Selezionare la sezione **Avanzate**
- Selezionare la scheda **Rete** -> **Connessioni**
- Cliccare su **Impostazioni** e selezionare l'opzione **Nessun Proxy**.

Google Chrome

- Avviare il browser Google Chrome.
- Cliccare sull'icona e selezionare la voce **Opzioni**.
- Selezionare la scheda Roba da Smanettoni e successivamente l'opzione **Rete** -> **Modifica impostazioni Proxy**.

A questo punto è necessario lanciare Internet Explorer, andare nel menù **Strumenti**, poi scegliere la sezione **Connessioni** e spuntare una delle seguenti voci:

- Non utilizzare mai connessioni remote
- Usa connessione remota se non è disponibile una connessione di rete

1.8 Configurazione TCP/IP

Configurazione del PC in Windows 2000

- Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections.**
- Cliccare due volte su **Local Area Connection.**
- In **Local Area Connection Status/Wireless** cliccare **Properties.**
- Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties.**
- Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically.**
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows XP

- Andare su **Start** e poi **Panello di Controllo**. Cliccare due volte su **Connessione di rete** (se non fosse presente cliccare prima su: **Passa alla Visualizzazione Classica**).
- Cliccare due volte su **Connessione alla rete locale (LAN)/Wireless.**
- Nel TAB generale cliccare **Proprietà**.
- Selezionare **Protocollo Internet (TCP/IP)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente.**
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows Vista

- Andare su **Start** poi **Pannello di Controllo** (cliccare sulla voce **Visualizzazione classica**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione, poi** cliccare su **Gestisci connessione di rete.**
- Cliccare 2 volte sull'icona **Local Area Connection/Wireless** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).
- Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in Windows 7

- Andare su **Start** poi **Pannello di Controllo** (cliccare sulla voce **Icone Piccole o Grandi**) e qui cliccare due volte sull'icona **Centro Connessione di rete e Condivisione,** poi cliccare su **Modifica Impostazione Scheda.**
- Cliccare 2 volte sull'icona **Local Area Connection/Wireless** e cliccare su **Proprietà** poi cliccare su **Continua** (per continuare è necessaria l'utorizzazione dell'utente).
- Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà.**
- Selezionare l'opzione **Ottieni automaticamente un indirizzo IP** e successivamente **Ottieni indirizzi server DNS automaticamente**.
- Premere su **OK** per terminare la configurazione.

Configurazione del PC in MAC OS

- Cliccare sull'icona **Mela** nell'angolo in alto a sinistra dello schermo e selezionare: **Control Panel/TCP/IP**. Apparirà la finestra relativa al TCP/IP come mostrata in figura.
- Scegliere **Ethernet** in Connect Via.
- Scegliere **Using DHCP Server** in Configure.

Lasciare vuoto il campo **DHCP Client ID**.

2. Configurazione del WebShare 242WN

2.1 Parametri di abbonamento

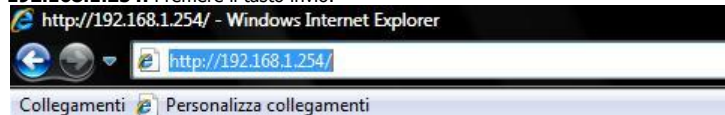
Prima di approcciare alla configurazione del WebShare Torrent 242 WN, è necessario essere in possesso di alcuni parametri fondamentali relativi all'abbonamento ADSL in proprio possesso.

	Le credenziali di accesso alla rete possono essere fornite esclusivamente dall'ISP con il quale è stato sottoscritto l'abbonamento ADSL. Il Supporto Tecnico Atlantis non può in alcun modo essere a conoscenza di tali parametri né può fornire alcun supporto in merito alla configurazione del prodotto nel caso in cui l'utente non sia a conoscenza di questi ultimi.

PROTOCOLLO	INFORMAZIONI NECESSARIE
PPPoE	VPI and VCI VC-based / LLC-based multiplexing Username and Password Service Name
PPPoA	VPI and VCI VC-based / LLC-based multiplexing Username and Password
RFC1483 Bridged	VPI/VCI VC-based / LLC-based multiplexing
RFC1483 Routed	VPI/VCI VC-based / LLC-based multiplexing IP address Subnet mask Default Gateway (IP address) IP address (DNS)

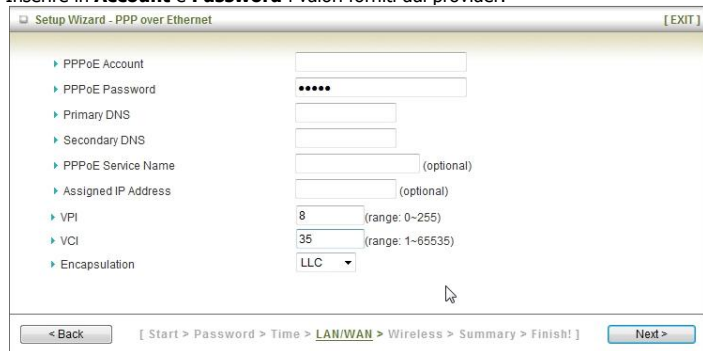
Nel caso in cui tali parametri non siano stati comunicati o siano stati smarriti, si prega di verificare questi dati con il proprio fornitore di servizi ADSL.
A questo punto è possibile configuare la sezione ADSL del WebShare (taluni provider non controllano username e password, quindi è probabile che il dispositivo già consenta la navigazione).

2.2 Configurazione Tramite WEB

Accedere col browser web al seguente indirizzo IP che di default è: **192.168.1.254.** Premere il tasto invio.

Utilizzare **admin** (come nome utente) e **atlantis** (come password). Cliccare poi su **Login** per continuare.
Cliccare su **Wizard** in alto **(**oppure spuntare la voce **Wizard Setup** e cliccare su **Enter).** La procedura di Wizard si articola in pochi semplici passaggi e può essere terminata in qualche minuto. Cliccare **Next** per iniziare

	Se si desidera una configurazione completa, per cui si rimanda al manuale presente su disco, cliccare sulla voce **Advanced Setup.**

	Il dispositivo potrebbe richiedere un nuovo login se durante la Wizard la password di accesso venisse cambiata.

Nella prima schermata è possibile cambiare la password di accesso al dispositivo (questa password è quella di accesso alla sezione WEB del router da non confondere con quella di autenticazione per il servizio ADSL dell'ISP). Digitare la vecchia password (atlantis) e poi 2 volte quella nuova. Cliccare su **Next** per procedere. Nella seconda schermata è possibile impostare il fuso orario appropriato dalla combo-box. Cliccare su **Next** per procedere. A questo punto è necessario scegliere il protocollo del proprio abbonamento ISP. Spuntare la voce **Setup WAN Type Manually** e cliccare poi su **Next.**
Nella schermata seguente selezionare **ADSL WAN** nella combo Box **WAN Interface.**

Selezionare in **WAN Type:**

- **PPPo over ATM** in caso di abbonamento con username e password del tipo **PPPoA (RFC2364).** Passare alla sezione **PPPoA/PPPoE.**
- **PPPo over Ethernet** in caso di abbonamento con username e password del tipo **PPPoE (RFC2516).** Passare alla sezione **PPPoA/PPPoE.**
- **IP over ATM (RFC 1483 Routed)** nel caso di abbonamento con IP statico del tipo RFC 1483 Routed. Passare alla sezione **Static IP Address.**

cliccare poi su **Next.**

PPPoE/PPPoA

PPPoE/PPPoA sono connessioni ADSL conosciute come dial-up DSL. Sono state concepite per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento e condividere lo stesso account con più PC.
Inserire in **Account** e **Password** i valori forniti dal provider.

Introdurre nei primi 2 campi rispettivamente Username/Password forniti dall'ISP.
Verificare che i parametri siano, nel caso di **PPPoE**, quelli in figura (**VPI=8**, **VCI=35**, **Encapsulation=LLC)** ove non specificatamente indicato dall'ISP.
Nel caso di **PPPoA** invece verificare che i parametri siano (**VPI=8**, **VCI=35**, **Encapsulation=VC-Mux**), ove non specificatamente indicato dall'ISP.
Cliccare a questo punto su **Next** sino al completamento della procedura guidata (passare alla sezione Wireless Setting).

Static IP Address

Questa configurazione è valida nel caso di abbonamento con 1 IP statico e dunque NAT attivo (per la gestione della classe pubblica fare riferimento al manuale su CD).
Spuntare in **IP Mode** la voce **Static IP Address** e digitare poi l' **indirizzo IP pubblico statico assegnato dall'ISP** e successivamente la **Subnet Mask**, **l'ISP Gateway** ed i **DNS.**
Verificare che i parametri siano (**VPI=8**, **VCI=35**, **Encapsulation=LLC**), ove non specificatamente indicato dall'ISP.

Cliccare a questo punto su **Next** sino al completamento della procedura guidata.

	Qualora si fosse cambiata la password di accesso, il dispositivo potrebbe richiedere un nuovo login.

Wireless Setting

Non resta adesso che cambiare eventualmente la configurazione della sezione wireless (cambiando SSID e tipologia di autenticazione).

Setup Wizard - Wireless settings [EXIT]

- Wireless Module: Enable / Disable
- Network ID(SSID): A02-RAU242-WN
- Channel: 6

< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Next >

Setup Wizard - Wireless settings [EXIT]

- Authentication: WPA2-PSK
- Encryption: AES
- Preshare Key: WebShare242WN

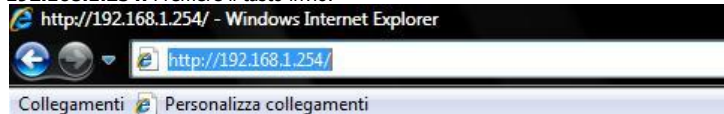
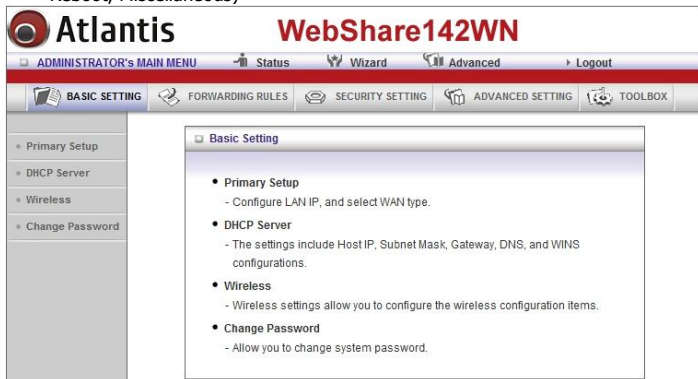
< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Next >

Il dispositivo mostrerà una schermata riassuntiva, cliccare su **Apply Settings** una volta verificata la correttezza delle impostazioni. Una volta effettuato il riavvio il led WAN dovrebbe essere verde fisso (può essere necessario qualche minuto).
Buona navigazione.

	Qualora venisse mostrata una schermata con l'errore **Connect to Internet Fail**, cliccare il bottone **Connect Again** (il tempo di allineamento può richiedere più tempo del previsto e generare questo errore di time-out). Il dispositivo mostrerà una schermata con tutti i parametri della WAN (tipo di linea, indirizzo IP). Cliccare su **Finish.**

3. Configurazione Avanzata via WEB

3.1 Configurazione Tramite WEB

Accedere col browser web al seguente indirizzo IP che di default è: **192.168.1.254.** Premere il tasto invio.

Verrà visualizzata la schermata di sotto:

Utilizzare **admin** come user ed **atlantis** (come password). Premere **Login** per continuare.

Selezionare **Advanced Setup** e cliccare poi su **Enter** (oppure cliccare direttamente su **Advanced**).

Apparirà a questo punto il Menù Principale, nella cui parte superiore verranno visualizzate (come se si stessero vedendo i links in una homepage) tutte le sezioni disponibili:

- **Basic Setting** (Network Setup, DHCP Server, Wireless, Change Password)
- **Forwarding Rules** (Virtual Server, Special AP, Miscellaneous)
- **Security Setting** (Status, Packet Filters, Domain Filters, URL Blocking, Mac Control, Miscellaneous)
- **Advanced Setting** (Status, System Log, Dynamic DNS, QoS, SNMP, Routing, System Time Scheduling)
- **NAS** (Disk Utility, File Sharing, Access Control, iTunes Server, Download Assistant, Download Status, Web HDD)
- **ToolBox** (System Info, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, Miscellaneous)

Al momento dell'accesso all'interfaccia di configurazione e gestione del dispositivo, verrà mostrata un'interfaccia che garantisce il pieno controllo ed il più alto livello di configurabilità possibile.
Per comodità di consultazione, da questa sezione nel manuale verrà trattata la sola sezione **Advanced** mentre all'interno della guida rapida (o nei primi 2 capitoli di questo manuale) verrà trattata la **Wizard**;

	Se si desidera utilizzare la Configurazione Rapida, spuntare la voce **Wizard** e poi cliccare su **Enter.** Maggiori dettagli al paragrafo 2.2.

Nella barra **ADMINISTRATOR's MAIN MENU** sono disponibili 4 voci:

- **Status:** permette di avere un quadro d'insieme del dispositivo
- **Wizard:** permette l'avvio del Wizard di configurazione
- **Advanced:** (dalla sez 3.2 in avanti)
- **Logout:** (per effettuare il Logout dal sistema)

Status

Parametro	Descrizione
System Status	Sono contenute informazioni circa l'indirizzo della WAN e lo stato del modulo ADSL.
Wireless Status	Sono contenute informazioni circa il funzionamento del modulo Wireless.
Statistics Information	Sono contenute informazioni circa i pacchetti inviati attraverso la WAN.
Peripheral Status	Viene mostrato la periferica USB di memorizzazione. Le periferiche riconosciute devono avere **status=Ready**.
ADSL Modem Status	Permette di accedere alla sezione del modulo ADSL, dove è possibile avere dettagli sulla linea in uso.
View Log	Cliccare per avere accesso ai log di sistema.
Client List	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Nat Status	Cliccare per accedere alla tabella di NAT.
Refresh	Cliccare per aggiornare la pagina.

	Quando si connette una periferica USB 3G, viene aggiunta una sezione in cui sono contenuti dettagli circa il riconoscimento e funzionamento della periferica.

3.2 Basic Setting

Network Setup

LAN Setup

Item	Setting
LAN IP Address	192.168.5.60
Subnet Mask	255.255.255.0

Parametro	Descrizione
LAN IP Address	Inserire l'indirizzo IP da assegnare all'interfaccia LAN del prodotto. La radice dell' indirizzo verrà utilizzata anche per l'assegnazione del range DHCP.
Subnet Mask	Digitare la subnet Mask.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

In questa sezione è possibile configurare i profili di connessione per l'interfaccia ADSL.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.
In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

Le credenziali di accesso alla rete possono essere fornite esclusivamente dall'ISP con il quale è stato sottoscritto l'abbonamento ADSL. Il Supporto Tecnico Atlantis non può in alcun modo essere a conoscenza di tali parametri né può fornire alcun supporto in merito alla configurazione del prodotto nel caso in cui l'utente non sia a conoscenza di questi ultimi.
Prima di procedere è opportuno consocere la tipologia di contratto fornita dall'ISP.

Prima di configurare la connessione è opportuno considerare che WebShare 242WN è dotato di una doppia interfaccia WAN di connessione ADSL2+/3G; ognuna di esse può essere impostata come singola connessione primaria (Single-WAN). Nel caso si scelga la configurazione Dual-WAN è invece possibile permettere il backup della connessione primaria nel caso di failover temporaneo della linea ADSL, garantendo cosi una connessione sempre attiva.

	Nella modalità DUAL WAN alla porta USB deve essere connesso un modem USB 3G (non incluso).

ADSL - PPPoE Connection

PPPoE è una connessione ADSL conosciuta come dial-up DSL. Al pari del PPPoA e' stata concepita per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento e condividere lo stesso account con l'ISP. Non è richiesto alcun software aggiuntivo.
Selezionare **WAN Interface=ADSL WAN** e **WAN TYPE= PPP over Ethernet.**

Internet Setup	[HELP]
WAN Interface	ADSL WAN
WAN Type	PPP over Ethernet
Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:
PPPoE Account	
PPPoE Password	
Primary DNS	
Secondary DNS	
Connection Control	Auto Reconnect (always-on)
Maximum Idle Time	600 seconds
PPPoE Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT disable	Enable
Data Encapsulation	LLC
VPI Number	8 (range: 0~255)
VCI Number	35 (range: 1~65535)
Schedule type	UBR
Save Undo	

Parametro	Descrizione
Activate WWAN for Auto-Failover	Spuntare **Enable** per attivare l'autofailover su scheda USB 3G qualora la linea ADSL sia in down. La verifica viene fatta effettuando un ping verso **Remote Host for keep alive. E' pertanto opportuno introdurre un indirizzo IP di un sito che è sempre attivo. Se questo sito dovesse risultare down il sistema attiverà la modalità backup anche se l'adsl è funzionante.**
PPPoE Account	Fornita dall'ISP, tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
PPPoE Password	Fornita dall'ISP, tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
PrimaryDNS	Inserire l'IP del DNS. Lasciare 0.0.0.0 per riceverlo automaticamente dall'ISP.
Secondary DNS	Inserire l'IP del DNS. Lasciare 0.0.0.0 per riceverlo automaticamente dall'ISP.
Connection Control	Sono disponibili 3 strategie di connessione: Auto Reconnect: ▪ **Connect-on-demand:** Il router costruirà la connessione PPP solo quando rileva pacchetti verso internet. ▪ **Auto Reconnect (Always-on):** La connessione è mantenuta sempre attiva. ▪ **Manually:** Nella pagina di Status la connessione va manualmente attivata. Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.
Maximum Idle Time	Definire il tempo, in secondi, di non attività prima che la sessione venga abbattuta.
PPPoE Service Name	Lasciare vuoto se non espressamente comunicato dall'ISP. E' un identificativo, può essere richiesto da alcuni ISP. Al solito può essere composto da massimo 63 caratteri (case sensitive) alfanumerici.
Assigned IP	Lasciare 0.0.0.0 per ottenere automaticamente l'indirizo IP

	dall'ISP, in caso contrario inserire l'indirizzo IP fisso.
MTU	Indica le dimensioni massime del datagramma transitante sull'interfaccia.
NAT Disable	Spuntare(per disattivare il NAT) solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge. Di default è **NON spuntato.**
Data Encapsulation	Selezionare **LLC** se non diversamente indicato dall'ISP.
VPI Number	Scrivere il numero di VPI. IL valore di default è **8**. Lasciare tale valore se non diversamente indicato dall'ISP.
VCI Number	Scrivere il numero di VCI. IL valore di default è **35**. Lasciare tale valore se non diversamente indicato dall'ISP.
Schedule Type	Selezionare il valore di Quality of Server per la tratta ATM. Lasciare il valore di default.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
Reboot	Cliccare per effettuare un reboot del dispositivo. Condizione necessaria affinché i nuovi settaggi siano utilizzati.

	Se la navigazione avviene senza problemi ma l'invio di allegati nelle mail crea problemi, potrebbe rendersi necessaio cambiare l'MTU abbassandone il valore in 1450 (anziché il valore 1492 di default).

ADSL - PPPoA Connection

PPPoA è una connessione ADSL conosciuta come dial-up DSL. Al pari del PPPoA e' stata concepita per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento e condividere lo stesso account con l'ISP. Non è richiesto alcun software aggiuntivo.
Selezionare **WAN Interface=ADSL WAN** e **WAN TYPE= PPP over ATM.**

Internet Setup	[HELP]
WAN Interface	ADSL WAN
WAN Type	PPP over ATM
Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:
PPPoA Account	
PPPoA Password	•••••
Primary DNS	
Secondary DNS	
Connection Controll	Auto Reconnect (always-on)
Maximum Idle Time	600 seconds
Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT disable	Confirm
Data Encapsulation	VCMux
VPI Number	8 (range: 0~255)
VCI Number	35 (range: 1~65535)
Schedule type	UBR
Save Undo	

Parametro	Descrizione
Activate WWAN for Auto-Failover	Spuntare **Enable** per attivare l'autofailover su scheda USB 3G qualora la linea ADSL sia in down. La verifica viene fatta effettuando un ping verso **Remote Host for keep alive.** **E' pertanto opportuno introdurre un indirizzo IP di un sito che è sempre attivo.** **Se questo sito dovesse risultare down il sistema attiverà la modalità backup anche se l'adsl è funzionante.**
PPPoA Account	Fornita dall'ISP, tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
PPPoA Password	Fornita dall'ISP, tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.
PrimaryDNS	Inserire l'IP del DNS. Lasciare 0.0.0.0 per riceverlo automaticamente dall'ISP.
Secondary DNS	Inserire l'IP del DNS. Lasciare 0.0.0.0 per riceverlo automaticamente dall'ISP.
Connection Control	Sono disponibili 3 strategie di connessione: Auto Reconnect: ▪ **Connect-on-demand:** Il router costruirà la connessione PPP solo quando rileva pacchetti verso internet. ▪ **Auto Reconnect (Always-on):** La connessione è mantenuta sempre attiva. ▪ **Manually:** Nella pagina di Status la connessione va manualmente attivata. Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.
Maximum Idle Time	Definire il tempo, in secondi, di non attività prima che la sessione venga abbattuta.
Service Name	Lasciare vuoto se non espressamente comunicato dall'ISP. E' un identificativo, può essere richiesto da alcuni ISP. Al solito può essere composto da massimo 63 caratteri (case sensitive) alfanumerici.
Assigned IP	Lasciare 0.0.0.0 per ottenere automaticamente l'indirizo IP

	dall'ISP, in caso contrario inserire l'indirizzo IP fisso.
MTU	Indica le dimensioni massime del datagramma transitante sull'interfaccia.
NAT Disable	Spuntare(per disattivare il NAT) solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge. Di default è **NON spuntato.**
Data Encapsulation	Selezionare **VCMux** se non diversamente indicato dall'ISP.
VPI Number	Scrivere il numero di VPI. IL valore di default è **8**. Lasciare tale valore se non diversamente indicato dall'ISP.
VCI Number	Scrivere il numero di VCI. IL valore di default è **35**. Lasciare tale valore se non diversamente indicato dall'ISP.
Schedule Type	Selezionare il valore di Quality of Server per la tratta ATM. Lasciare il valore di default.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
Reboot	Cliccare per effettuare un reboot del dispositivo. Condizione necessaria affinché i nuovi settaggi siano utilizzati.

	Se la navigazione avviene senza problemi ma l'invio di allegati nelle mail crea problemi, potrebbe rendersi necessaio cambiare l'MTU abbassandone il valore in 1450 (anziché il valore 1492 di default).

ADSL – RFC1483 Routed (IP Over ATM)

Utilizzare in caso di IP Statico con protocollo RFC 1483. Per dettagli ulteriori si consulti l'appendice **Classe Pubblica.**
Selezionare **WAN Interface=ADSL WAN** e **WAN TYPE= IP Over ATM (RFC 1483 Routed)**

Internet Setup	[HELP]
WAN Interface	ADSL WAN
WAN Type	IP over ATM (RFC 1483 Routed)
Activate WWAN for Auto-Failover	☐ Enable Remote Host for keep alive:
IP Mode	Static IP Address
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
NAT disable	☐ Enable
Data Encapsulation	LLC
VPI Number	8 (range: 0~255)
VCI Number	35 (range: 1~65535)
Schedule type	UBR
	Save Undo

Parametro	Descrizione
Activate WWAN for Auto-Failover	Spuntare **Enable** per attivare l'autofailover su scheda USB 3G qualora la linea ADSL sia in down. La verifica viene fatta effettuando un ping verso **Remote Host for keep alive.** **E' pertanto opportuno introdurre un indirizzo IP di un sito che è sempre attivo.** **Se questo sito dovesse risultare down il sistema attiverà la modalità backup anche se l'adsl è funzionante.**

IP Mode	A seconda della modalità scelta in **IP Mode** ci potrà essere: ▪ **Static IP Address** (inserito in fase di configurazione) ▪ **Dynamic IP Address** (fornito dall'ISP). In questo caso è possibile utilizzare i campi **Host Name** e **ISP Registered MAC Address** (nel caso in cui l'IP sia assegnato dall'ISP solo ad un determinato MAC). IP Mode: Dynamic IP Address Host Name: (optional) ISP registered MAC Address: Clone
WAN IP Address	Inserire l'indirizzo IP fisso fornito dal provider.
WAN Subnet Mask	Inserire la maschera di rete relativa all'indirizzo IP impostato nel campo IP.
WAN Gateway	Inserire l'indirizzo Gateway per l'instadamento del traffico WAN verso Internet.
PrimaryDNS	Inserire l'IP del DNS.
Secondary DNS	Inserire l'IP del DNS.
NAT Disable	Spuntare(per disattivare il NAT) solo in caso si possieda una classe pubblica o se il prodotto viene fatto funzionare come Bridge. Di default è **NON spuntato.**
Data Encapsulation	Selezionare **LLC** se non diversamente indicato dall'ISP.
VPI Number	Scrivere il numero di VPI. IL valore di default è **8**. Lasciare tale valore se non diversamente indicato dall'ISP.
VCI Number	Scrivere il numero di VCI. IL valore di default è **35**. Lasciare tale valore se non diversamente indicato dall'ISP.
Schedule Type	Selezionare il valore di Quality of Server per la tratta ATM. Lasciare il valore di default.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Wireless WAN

Anzitutto è opportuno collegare una scheda 3G supportata alla porta USB del WebShare 242WN e controllare in Status che questa venga correttamente riconosciuta ed installata.
A questo punto è possibile passare alla configurazione dei parametri di connessione.
Selezionare **WAN Interface=Wireless WAN** e **WAN TYPE= 3G.**

Internet Setup	[HELP]
WAN Interface	Wireless WAN
WAN Type	3G
Dial-Up Profile	Auto-Detection Manual
PIN Code	(optional)
Connection Control	Auto Reconnect (always-on) Maximum Idle Time 600 seconds
Allowed Connection Time	Always By Schedule
MTU	0 (0 is auto)
Keep Alive	Disable LCP Echo Request Interval 10 seconds Max Failure Time 3 times Ping Remote Host Host IP Interval 60 seconds
	Save Undo

Parametro	Descrizione
Dial-UP Profile	Selezionare **Auto-Detection** per permettere al sisteme una configurazione automatica, in caso di problemi selezionare **Manual.**
Pin Code	Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo PIN.
Connection Control	Sono disponibili 3 strategie di connessione: Auto Reconnect: ▪ **Connect-on-demand:** Il router costruirà la connessione PPP solo quando rileva pacchetti verso

	internet. ▪ **Auto Reconnect (Always-on):** La connessione è mantenuta sempre attiva. ▪ **Manually:** Nella pagina di Status la connessione va manualmente attivata. Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato. In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.
Maximum Idle Time	Definire il tempo, in secondi, di non attività prima che la sessione venga abbattuta.
Allowed Connection Time	Spunatre **Always** per non inserire alcun vincolo orario alla connessione. Spunatre invece **By Scheduled** (selezionare poi una regola) per inserire vincoli orari.
MTU	Indica le dimensioni massime del datagramma transitante sull'interfaccia.
Keep Alive	Selezionare attraverso quale modalità il Router effettuerà la diagnostica del corretto funzionamento della connessione primaria. Sono disponibili 3differenti opzioni: ▪ **Disable:** Non viene effettuato alcuna verifica. ▪ **LCP ECHO REQUEST:** digitare in **Interval** il tempo in secondi fra 2 pacchetti LCP, mentre in **Max Failure Time** digitare il numero di fallimenti accettati. ▪ **Ping Remote Host:** digitare in **Interval** il tempo in secondi fra 2 ping, mentre in **Host IP** l'indirizzo IP del server**.**
Secondary DNS	Inserire l'IP del DNS. Lasciare 0.0.0.0 per riceverlo automaticamente dall'ISP.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Selezionando **Dial-UP Profile=Manual** dovranno essere inserite le seguenti informazioni:

- **Country**:selezionare la regione dove il dispositivo è utilizzato.
- **Telecom:** selezionare il Provider. Qualora questo non ci fosse selezionare **Others.**
- **3G Network:** selezionare la tipologia di network.
- **APN:** digitare l'APN del proprio ISP.
- **PIN Code:** Nel caso in cui la SIM card sia protetta dal codice di sicurezza PIN, immettere questo valore nel campo PIN**.**
- **Dialed Number:** in genere è ***99#**
- **Account/password/Authentication:** selezionare la tipologia di autenticazione ed il profilo.
- **Primary/secondary DNS:** immettere i DNS del proprio ISP

er alcune particolari tipologie di contratto poco recenti, la registrazione al servizio 3G può essere attivata manualmente richiedendo il servizio direttamente al proprio operatore di telefonia mobile.
In questi casi è possibile che il valore del campo APN vada variato in **uni.tim.it**
Per altri operatori l'APN può essere diverso:
Nel caso di Vodafone l'APN è **web.omnitel.it**
Nel caso di WIND l'APN è **internet.wind** o **internet.wind.biz**
Nel caso di TRE l'APN è **tre.it** o **datacard.tre.it**

Attenzione: L'immisione di un codice PIN errato per 3 volte porterà al blocco della SIM card.

Il modem 3G non è incluso nell'offerta ed andrà acquistato separatamente. Si prega di verificare la compatibilità del modem acquistato tramite la lista presente al termine di questo manuale o reperibile sul sito www.atlantis-land.com presso la sezione dedicata al prodotto.

	Attenzione: L'utilizzo del WebShare 242WN non è consigliato con abbonamenti con tariffazione basata sul tempo di connessione/traffico.

DHCP Server

DHCP Server [HELP]

Item	Setting
DHCP Server	Disable Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

Save | Undo | More... | Clients List... | Fixed Mapping...

DHCP

Parametro	Descrizione
DHCP	Se impostato su **Enable** il router assegnerà i parametri di rete ai DHCP client della LAN. Se impostato su **Disable** il server DHCP viene disabilitato. Quando la funzionalità DHCP è utilizzata è necessario impostare i parametri seguenti.
IP Pool Starting Address	Questo campo specifica il primo IP del pool di indirizzi che verranno assegnati agli host di rete.
IP Pool Starting Address	Questo campo specifica l'ultimo IP del pool di indirizzi che verranno assegnati agli host di rete.
Lease Time	Questo campo specifica il tempo di Lease degli indirizzi IP assegnati ai vari client.
Domain Name	Questo campo opzionale permette di introdurre il nome del dominio.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
More	Cliccare per introdurre gli IP dei server DNS/Gateway/WINS alternativi.
Client List	Cliccare per avere accesso alla lista dei client DHCP assegnati (con IP, MAC e Host Name). Selezionando una tupla e cliccando su Fixed Mapping è possibile creare un'associazione statica MAC-IP.
Fixed Mapping	Si faccia riferimento alle istruzioni seguenti.

Fixed Mapping: Sarà inoltre possibile configurare delle associazioni fisse per esigenze particolari (es: Server di rete). Per attivare tale funzionalità, selezionare l'opzione **Fixed Mapping** ed operare come segue:

Fixed Mapping [HELP]

DHCP clients -- select one -- Copy to ID --

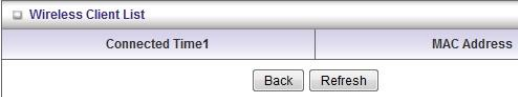
ID	MAC Address	IP Address	Enable
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

<<Previous Next>> Save Undo Back

Parametro	Descrizione
MAC Address	Indicare l'indirizzamento MAC del client che si desidera sottoporre a questa associazione statica.
IP Address	Indicare l'indirizzo IP che si intende associare al client.
Enable	Spuntare per attivare l'associazione.
DHCP Clients	Selezionare dalla lista gli IP assegnati dal router.
Copy To	Selezionare dalla combo List ID il numero di tupla doove creare l'associazione statica.
Next/Previous	Cliccare per scorrere tra le pagine
Save	Cliccare per salvare la configurazione su eprom.
Undo	Cliccare per cancellare gli ultimi dati inseriti.

Back	Cliccare per tornare alla pagina precedente.

Wireless

In questa sezione è possibile impostare tutti i parametri relative all'interfaccia wireless.
E' altresì possibile configurare fino a 4 link WDS (Wireless Distribution System) al fine di stabilire connessioni tra 2 o più Access Point. Per la configurazione di un link WDS, è necessario conoscere l'indirizzo MAC dell'Access Point al quale si desidera connettere il WebShare Router.

	La tecnologia WDS (Wireless Distribution System) non è sottoposta ad alcun standard specifico ed è sviluppata in maniera proprietaria dai vari produttori di chipset radio. Per queste motivazioni, connessioni WDS tra apparati differenti potrebbero presentare comportamenti anomali, fino alla mancata realizzazione della connessione tra gli stessi.

Wireless Setting [HELP]

Item	Setting
Wireless Module	Enable Disable
Transmit Power	50%
Network ID(SSID)	A02-RAU242-WN
SSID Broadcast	Enable Disable
Channel	6
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
Encryption	AES
Preshare Key	WebShare242WN

Save Undo WDS Setting...
WPS Setup... Wireless Client List...

Campo	Descrizione
Wireless	E' possibile abilitare o meno il modulo Wireless integrato. Spuntare **Enable** per attivare il modulo wireless.
Transmit Power	WebShare 242 WN è stato progettato per essere conforme alle normative vigenti nelle nazioni appartenenti alla Comunità Europea e anche a quelle in vigore negli stati extra CE. L'utente dovrà pertanto utilizzare il dispositivo senza mai cambiare il campo **TX Power Level (Advanced->Basic Setting->Wireless)** dal valore di default. Atlantis S.p.a. si solleva da qualsiasi responsabilità derivante da eventuali modifiche o utilizzo improprio del prodotto. Questo valore va aumentato a 100% solo nel caso in cui si sostituisse l'antenna fornita con una da 2 dBi (quella a corredo è da 5 dBi).
Network ID (SSID)	Inserire il nome identificativo da assegnare alla rete wireless.
SSID Broadcast	ESSID Broadcast è una funzione che permette di attivare/disattivare l'invio a tutti i client che ne facessero richiesta del valore ESSID identificativo della rete. Selezionare **Enable** per permettere che la rete venga visualizzata dai client durante le scansioni di ricerca, oppure **Disable** per rendere non visibile l'identificativo della rete.
Channel	Selezionare il canale da utilizzare per la trasmissione radio. Selezionare Auto per permettere al dispositivo di utilizzare il canale meno disturbato.
Wireless Mode	Selezionare la modalità di connessione tra le scelte proposte. Al fine di garantire un elevato grado di compatibilità con la maggior parte dei client, si consiglia di mantenere l'impostazione di default **Mixed Mode (b+g+n).** In caso si utilizzo con soli client wireless in standard b o g è possibile selezionare **11g only** o **11b only.**
Schedule Rule	Il modulo può essere fatto funzionare in determinati intervalli temporali. Si consulti la sezione **Rule Schedule.**
WDS Settings	E' altresì possibile configurare fino a 4 link WDS (Wireless Distribution System) al fine di stabilire connessioni tra 2 o più Access Point. Selezionare WEP in Security per abilitare il WDS. Si consulti la sezione seguente.
WPS Setup	Permette la configurazione della sicurezza della parte wireless in maniera semplice e rapida premendo l'apposito bottone.
Authentication	E' possibile impostare la sicurezza della rete Wireless. Si

Encryption Preshared Key	consulti la pagina seguente.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
Wireless Client List	Cliccare per accedere ad una schermata riassuntiva con l'elenco dei client in cui viene mostrato Tempo di connessione/MAC. Wireless Client List Connected Time1 | MAC Address Back Refresh

	▪ Il campo ESSID è case sensitive e non può superare il limite massimo di 32 caratteri ASCII. ▪ Atlantis consiglia la selezione di un canale non occupato, in quanto eventuali sovrapposizioni spaziali, temporali e di frequenza potrebbero indurre drastici cali in termini di performance.

	Ogni cambiamento al modulo wireless richiede un riavvio del dispositivo.

	Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11g/b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**". E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6). Da questo si evince che soltanto 3 Access Point/Wireles Router possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali (funzionamento contemporaneo).

	Nel caso si utilizzi lo standard IEEE802.11n i canali senza overlap sono solo 2 (basso/alto).

	Talune volte i il pacchetto DHCP non riesce a passare a cause di settaggi **RTS/CTS** e **Fragmentation Threshold(bytes).** Cambiare tali valori sulle configurazioni dei client. Riprovare verificando se l'attribuzione dell'indirizzo IP avviene correttamente.

Wireless Security

In questa sezione è possibile attivare un profile di crittografia al fine di proteggere la WLAN da accessi non desiderati. Il prodotto supporta i più avanzati criteri di protezione attualmente disponibili garantendo alcuna degradazione in termini di performance della rete wireless.
Di seguito sono riportate le configurazioni disponibili:

- **Open**
- **Shared**
- **WPA (WPA2)-PSK**
- **WPA/WAP2**

WEP (Wired Equivalent Privacy)

Authentication	Shared
Encryption	WEP
WEP Key 1	ASCII 1234567890
WEP Key 2	HEX 1234567890
WEP Key 3	HEX 1234567890
WEP Key 4	HEX 1234567890

Parametro	Descrizione
Authentication	Selezionare l'opzione **Shared**.
Encryption	Selezionare l'opzione **WEP**.
WEP Key 1-4	Selezionare la tipologia di chiave tra ASCII ed HEX. La lunghezza della chiave crittografica può essere a 64 o 128 bit a seconda della lunghezza della chiave inserita. Nella modalità HEX è necessario intrudurre 5 (WEP64), 13(WEP128) coppie di valori esadecimali [0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F]. Un esmpio di chiave a 64 bit può essere: "**0x**63B79B2FE7". Il carattere "0x" precede l'introduzione di una chiave HEX. Nella modalità ASCII è necessario intrudurre 5 (WEP64), 13 (WEP128) caratteri alfanumerici. E' possibile inserire 4 chiave ma solo una alla volta (quella selezionata) è utilizzata.

Il WEP non è oggi ritenuto sicura, si raccomanda di utilizzare il WPA-PSK.

WPA-PSK/ WPA2-PSK

Authentication	WPA-PSK
Encryption	TKIP
Preshare Key	WebShare242WN

Parametro	Descrizione
Security Mode	Selezionare l'opzione **WPA-PSK**, **WPA2-PSK** o **WPA/WPA2-PSK.**
Encryption	Scegliere il protocollo TKIP(WPA) o AES (WPA2). Il **TKIP** (Temporal Key Integrity Protocol) utilizza un sistema di rinnovo automatico delle chiavi ed offre pertanto (anche grazie al Message Integrity Code (MIC)) una maggiore sicurezza rispetto al protocollo WEP. L'**AES** invece cambia anche l'algoritmo di cifratura (prima era usato l'RC4) arrivando ad essere la soluzione più sicura. E' necessario che anche il client supporti il WPA-PSK(TKIP) o WPA2-PSK(AES).
WPA Shared Key	Inserire la chiave da utilizzare per la fase di autenticazione e crittografia dei dati.

WAP/WPA2

Security	WPA2
Encryption	TKIP AES
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

Save Undo Wireless Client List...

Parametro	Descrizione
Security Mode	Selezionare l'opzione **WPA**, **WPA2,WPA1/WPA2** o **802.11x and RADIUS.**
Encryption	Scegliere il protocollo TKIP(WPA) o AES (WPA2). Il **TKIP** (Temporal Key Integrity Protocol) utilizza un sistema di rinnovo automatico delle chiavi ed offre pertanto (anche grazie al Message Integrity Code (MIC)) una maggiore sicurezza rispetto al protocollo WEP. L'**AES** invece cambia anche l'algoritmo di cifratura (prima era usato l'RC4) arrivando ad essere la soluzione più sicura. E' necessario che anche il client supporti il WPA-PSK(TKIP) o WPA2-PSK(AES). Nel caso di **802.11x and RADIUS** scegliere la lunghezza in bit della chiave di cifratura.
RADIUS Server IP	Introdurre l'indirizzo IP del server Radius.
RADIUS Port	Introdurre la porta utilizzata dal server RADIUS, solitamente la 1882.
RADIUS Shared Key	Inserire la chiave da utilizzare per la fase di autenticazione e crittografia dei dati.

WPS

Il prodotto supporta pienamente le specifiche Wi-Fi Protected Setup, al fine di consentire una semplice installazione della rete wireless.
Questo insieme di specifiche prevede che le fasi di sincronizzazione e messa in sicurezza della WLAN vengano gestite in maniera autonoma dai dispositivi che supportino tali funzionalità.
Nello specifico, WPS prevede 2 modalità di sincronizzazione tra il punto di accesso ed i relativi client: la prima prevede la pressione di un apposito pulsante sul punto di accesso e successivamente su tutti i client appartenenti alla stessa wireless network. Questa procedura avvierà un processo di sincronizzazione automatica durante il quale i prodotti, oltre che all'autenticazione presso il punto di accesso, negozieranno una chiave di sicurezza (secondo gli standard supportati dai vari client) per la messa in sicurezza della rete. Al termine della procedura la rete wireless sarà così configurata e pronta per essere utilizzata.
La seconda prevede che la fase di autenticazione dei client sul punto di accesso avvenga tramite il riconoscimento di un codice PIN univoco associato al client, mentre tutta la parte successiva di messa in sicurezza sarà identica alla modalità illustrata sopra. Esistono 2 modalità di autenticazione (Enrollee o Registar) in base al dispositivo che si occuperà di gestire la fase iniziale di autenticazione.
Nello specifico, vediamo ora come configurare le 2 modalità di associazione WPS sul WebShare 142WN.

WPS Button Setup

- Premere il pulsante WPS posto sulla parte anteriore del WebShare Router; il led Wireless comincerà a lampeggiare in maniera regolare.
- Premere il pulsante WPS sul client o sui client che si desidera far autenticare al WebShare Router entro 120 secondi.

	In alcune tipologie di client, il pulsante WPS può non essere presente; si prega di consultare il manuale utente per la verifica del supporto di questa tecnologia e per l'eventuale modalità di attivazione.

WDS Setting

In questa sezione è possibile configurare i vari Link WDS utili ad estendere la copertura del sistema.

Wireless Bridging [HELP]

Item	Setting
Wireless Bridging	Enable Disable
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

Save Undo Back

Campo	Descrizione
Wireless Bridging	E' possibile abilitare o meno il modulo WDS integrato. Spuntare **Enable** per attivare tale modulo.
Remote AP MAC 1-4	Inserire l'indirizzo MAC remoto dell'AP con cui si desidera contruire il link WDS.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
Back	Cliccare per tornare alla schermata di configurazione Wireless.

	La tecnologia WDS (Wireless Distribution System) non è sottoposta ad alcun standard specifico ed è sviluppata in maniera proprietaria dai vari produttori di chipset radio. Per queste motivazioni, connessioni WDS tra apparati differenti potrebbero presentare comportamenti anomali, fino alla mancata realizzazione della connessione tra gli stessi.

	WebShare 242WN supporta il WDS solo in modalità WEP. Verificare che CANALE, SICUREZZA siano identiche a quelli dei dispositivi con cui si vuole costruire il link WDS.

Change Password

In questa sezione è possibile cambiare la password di accesso del dispositivo. E' fortemente consigliato effettuare un cambio di password al fine di rendere più sicuro l'accesso al dispositivo (unitamente alla configurazione ACL).

Change Password

Item	Setting
Old Password	
New Password	
Reconfirm	

Save Undo

Parametro	Descrizione
Old Password	Digitare la vecchia password.
New Password	Digitare la nuova password.
Reconfirm	Digitare ancora la nuova password per conferma.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Qualora si perdesse la password utilizzare la procedura di Reset per accedere nuovamente all'apparato.
Premendo il pulsante **WPS+Wireless ON/OFF** presente nel pannello posteriore del prodotto per 10 (o più) secondi, il router riporterà tutte le impostazioni ai valori iniziali.

3.3 Formwarding Rules

Il NAT del Router consente la protezione della LAN locale da parte di accessi esterni indesiderati. Può essere necessario comunque consentire ad utenti esterni l'accesso ad un PC specifico della Lan (per esempio verso un PC che offre funzionalità di server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta, su un PC della Lan interna. E' possibile scegliere la porta ed il protocollo che si intende rigirare sull'indirizzo IP privato.

Virtual Server

Questa funzionalità permette di impostare il Router in modo che un determinate tipo di traffico in arrive sull'interfaccia sterna (WAN) possa essere correttamente reindirizzato ad uno specifico indirizzo IP della rete LAN.
Molte delle applicazioni diffuse oggi in Internet (FTP Server, Web Hosting, etc), necessitano di una configurazione della sezione Port Forwarding in modo che le richieste provenienti da client esterni vengano correttamente inoltrare ai rispettivi server che si occuperanno di fornire una risposta a queste ultime.
Di seguito si riporta la procedura per la creazione di una nuova regola di port forwarding:

Virtual Server [HELP]

Well known services -- select one -- Copy to ID --

ID	Service Ports	Server IP	Enable	Use Rule#
1				(0) Always
2				(0) Always
3				(0) Always
4				(0) Always
5				(0) Always
6				(0) Always
7				(0) Always
8				(0) Always
9				(0) Always
10				(0) Always

Parametro	Descrizione
ID	Identificativo numerico fisso.
Server IP	Inserire l'indirizzo IP di un PC presente in LAN verso il quale indirizzare tutti i pacchetti che soddisfino la regola.
Service Port	Impostare la porta servizio verso la quale dovrà essere reindirizzato il pacchetto entrante che soddisfi la regola.
Enable	Spuntare per rendere attiva la regola.
Schedule (Use Rule #)	Selezionare il numero di regola temporale per impostare schedulazione della funzionalità. Per informazioni avanzate, fare riferimento al paragrafo relativo.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Il sistema permette un massimo di 20 regole.

	Utilizzando le combo-box nella parte superiore è possibile velocizzare il processo di creazione delle regole ed utilizzare settaggi reimpostati per alcuni servizi noti.

	Qualora l'opzione di NAT sia disabilitata la funzionalità di Virtual Server non è utilizzabile.

	Se sul Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual Server per evitare conflitti. In questo caso è sufficiente assegnare al PC Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Router ADSL) ed i server DNS) un indirizzo IP che sia nella stessa subnet del Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router.

	Il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range potrebbero sorgere problemi ed il servizio di VS funzionare in maniera impropria.

	Se l'applicazione non è inclusa nella lista **Well Know Services** di sopra, consultare il sito web del produttore dell'applicazione per conoscere le porte da ruotare. L'assistenza tecnica non fornirà dettagli sulle porte utilizzate dai vari software e/o applicativi che sono di esclusiva pertinenza della softwarehouse che ha sviluppato l'applicazione. Si invita pertanto a contattare tale softwarehouse.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del WebShare Router. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consultare eventuali aggiornamenti di questo manuale (scaricabile dal sito www.atlantis-land.com).

Applicazione	Connessioni Uscenti	Connessioni Entranti
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665-4672 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190
VNC	Nessuno	TCP 5900

Il Router può gestire un numero non infinito di connessioni, pertanto per grandi range (o centinaia di connessioni cintemporanee) potrebbero sorgere problemi.
Questo dispositivo supporta sino a 1500 connessioni contemporanee, quindi regolare i vari software di P2P affinché tale valore sia rispettato (in caso di dubbi chiamare l'assistenza tecnica).

Di seguito una serie di porte notevoli:

Servizio	Numero di Porta / Protocollo
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

Al fine di garantire una migliore comprensione di quanto trattato, di seguito un esempio di configurazione.
Si ponga di avere un server WEB attivo sulla propria rete LAN, ospitato su una macchina con indirizzamento IP 192.168.1.100; questo server deve essere in grado di rispondere alle richieste provenienti dai client esterni.

Posto che il gateway verso Internet per la macchina ospite del server WEB sia il WebShare 242WN, sarà necessario creare una regola di port forwarding come segue:

ID	Service Ports	Server IP	Enable	Use Rule#
1	80	192.168.1.100	☑	(0) Always

In questo caso, è stato possibile avvalersi di una delle regole reimpostate per reindirizzare il traffico HTTP verso il server 192.168.1.100

Special AP

Special Applications [HELP]

Popular applications -- Select one -- Copy to ID --

ID	Trigger	Incoming Ports	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐

Save Undo

Parametro	Descrizione
Trigger	Inserire le porte che in uscita abilitano il trigger. E' possibile abilitare particolari applicazioni, come i videgames, che richiedono connessioni multiple (generalmente critiche quando si usa il NAT).
Incoming Ports	Quando il trigger è attivo, le porte elencate possono attraversare il firewall.
Enable	Spuntare per rendere attiva la regola.

Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Il sistema permette un massimo di 8 regole.

Miscellaneous

Miscellaneous Items		[HELP]
Item	Setting	Enable
IP Address of DMZ Host		☐
UPnP setting		☑
Save Undo		

Parametro	Descrizione
Internal Address of DMZ Host	Un PC sottoposto a DMZ è a tutti gli effetti un computer esposto ad Internet; in questa configurazione, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server). Sarà possibile impostare un solo indirizzo IP come DMZ Host in quanto tutto il traffico che non sia in grado di soddisfare una regola di Port Forwarding verrà indirizzato verso questo client. Per la configurazione, è necessario solamente spuntare il campo **Enabled** ed inserire nel campo **Internal Address of DMZ Host** l'indirizzamento dell'host DMZ (Sarà possibile selezionarlo altresì dalla lista a scomparsa).
UPnP setting	Abilita o disabilita il supporto Universal Plug'n'Play. Questa tecnologia permette, se supportata dall'applicazione, la creazione di regole dinamiche di port-forwarding in modo da garantire il corretto funzionamento dell'applicativo utilizzato (es: Windows Live Messenger).
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Se abilitata, la funzionalità DMZ consente la rotazione di tutti i protocolli verso un determinato indirizzo IP privato della Lan. Può essere abilitata per consentire il passaggio di determinati servizi. Resta inteso che una DMZ è una falla per la sicurezza, va pertanto utilizzata per reali necessità.

3.4 Security Setting

Status

In questa sezione è possibile avere un quadro d'insieme immediato dello stato di funzionamento dei vari moduli nel Firewall.

Outbound Filter [Modify]

Item	Status		
Outbound Filter	The below local clients just deny remote services as follows :		
Local Client	Only Allow Remote Host	Service	Working Time

Inbound Filter [Modify]

Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time

Domain Filter [Modify]

Item	Status
Domain Filter	Disable
Domain	Access
All other Domains	Yes

Refresh

Parametro	Descrizione
Modify	Cliccare per modificare la sezione opportuna.
Refresh	Cliccare per aggiornare la pagina.

Packet Filters

Queste funzioni di filtraggio dei pacchetti IP sono in buona sostanza una serie di regole che il Router applicherà ai pacchetti IP che lo attraversano. E' utile comunque sapere che il solo filtraggio sui pacchetti non elimina i problemi legati a livello di applicazioni o altri livelli.
Le politiche con cui organizzare il filtraggio sono essenzialmente riassumibili in 2 differenti filosofie:

- Passa solo quello che ritengo sicuro il resto è bloccato
- Blocco quello che ritengo pericoloso e tutto il resto passa.

Tali politiche dovrebbe essere applicata da coloro che possiedono una buona conoscenza di Internet (in particolar modo nel primo approccio) in quanto è necessario creare una regola per ogni "servizio" che si vuole usare.

Inbound Packet Filter [HELP]

Item	Setting
Inbound Filter	Enable

Allow all to pass except those match the following rules.
Deny all to pass except those match the following rules.

Schedule rule (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1		:		0
2		:		0
3		:		0
4		:		0
5		:		0
6		:		0
7		:		0
8		:		0

Save Undo Outbound Filter... MAC Level...

Parametro	Descrizione
Inbound Filter	Spuntare **Enable** per abilitare il modulo di filtraggio sui

Outbound Filter	pacchetti entranti o uscenti. Cliccare il bottone nella parte bassa della schermata per ruotare tra i 2 moduli presenti.
Allow all to pass except those match the following rules	Spuntare per Bloccare quello che ritengo pericoloso (e che verrà esplicitato nelle 8 regole di sotto) e tutto il resto passa.
Deny all to pass except thoe match the following rules	Spuntare per permettere il passaggio solo quello che ritengo sicuro (e che verrà esplicitato nelle 8 regole di sotto) e tutto il resto è bloccato.
ID	Identificativo numerico di regola.
Source IP	Inserire l'indirizzo di provenienza del pacchetto. E' possibile inserire un range digitando i 2 IP separati dal trattino "-".
Destination IP/Ports	Inserire l'indirizzo/porta destinazione del pacchetto. Iserire il prefisso T per TCP ed U per UDP davanti al numero di porta. Nessun prefisso implica entrambi i protocolli. Per indicare un intervallo di porte è possibile inserire un range digitando i 2 valori separati dal trattino "-". Esempio: **U1000-1999**, blocca le porte UDD dalla 1000 alla 1999.
Enable	Spuntare per rendere attiva la regola.
Schedule	Selezionare il numero di regola temporale per impostare schedulazione della funzionalità. Per informazioni avanzate, fare riferimento al paragrafo relativo.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Il sistema permette un massimo di 16 regole divise in 8 per modulo (Inbound/Outbound).

	Si consiglia la lettura dell'Appendice C.

Domain Filters

Le politiche con cui organizzare il filtraggio sono essenzialmente riassumibili in 2 differenti filosofie:

- Blocco i domini indicati e permetto l'accesso a tutto ciò che non è esplicitamente dichiarato.
- Consento l'accesso esclusivamente ai domini dichiarati e blocco tutto il resto.

Nello specifico, di seguito verranno indicate entrambe le filosofie di filtering, cosi da poter fornire un'ampia gamma di soluzioni anche all'utilizzatore più esperto.

Domain Filter [HELP]

Item	Setting
Domain Filter	Enable
Log DNS Query	Enable
Privilege IP Addresses Range	From 0 To 0

ID	Domain Suffix	Action	Enable	Schedule Rule#
1		Drop Log		0
2		Drop Log		0
3		Drop Log		0
4		Drop Log		0
5		Drop Log		0
6		Drop Log		0
7		Drop Log		0
8		Drop Log		0
9		Drop Log		0
10	* (all others)	Drop Log	-	0

Save Undo

Parametro	Descrizione
Domain Filter	Spuntare **Enable** per abilitare il modulo Domain Filter.
Log DNS Query	Spuntare **Enable** per abilitare la funzionalità di LOG.
Privilege IP Addresses Range	Digitare il range di IP esclusi da questo filtraggio.

Domain Suffix	Digitare il suffisso o dominio completo da bloccare.
Action	E' possibile permettere il passaggio (spuntare **LOG**) oppure il Blocco del pacchetto in esame (**Drop**).
Enable	Spuntare per rendere attiva la regola.
Schedule	Selezionare il numero di regola temporale per impostare schedulazione della funzionalità. Per informazioni avanzate, fare riferimento al paragrafo relativo.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Il sistema permette un massimo di 10 regole.

URL Blocking

Tramite questa funzionalità è possibile filtrare ulteriormente il traffico in uscita limitando tale traffico in base all'ora e/o giorno, al tipo di URL (una determinata sequenza di caratteri) e ad una parola contenuta all'interno dell'URL stessa.

URL Blocking [HELP]

Item	Setting
URL Blocking	☐ Enable

ID	URL	Enable
1		☐
2		☐
3		☐
4		☐
5		☐
6		☐
7		☐
8		☐
9		☐
10		☐

Save Undo

Parametro	Descrizione
Eanble	Spuntare per abilitare il modulo di URL Blocking.
URL	Se una parte dell'URL di un determinato sito include le parole inserite questa vie bloccata.
Enable	Spuntare per rendere attiva la regola.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

	Il sistema permette un massimo di 10 regole.

Mac Control

MAC Address Control [HELP]

Item	Setting
MAC Address Control	☐ Enable
☐ Connection control	Wireless and wired clients with C checked can connect to this device; and allow ▾ unspecified MAC addresses to connect.
☐ Association control	Wireless clients with A checked can associate to the wireless LAN; and deny ▾ unspecified MAC addresses to associate.

DHCP clients -- select one -- ▾ Copy to ID -- ▾

ID	MAC Address	C	A
71		☐	☐
72		☐	☐
73		☐	☐
74		☐	☐
75		☐	☐

<<Previous Next>> Save Undo

Parametro	Descrizione
Mac Address Control	Spuntare **Enable** per abilitare il modulo di filtraggio sui MAC.
Connection Control	Spuntare **Connection Control** per abilitare il modulo di filtraggio sui MAC dei soli dispositivi Wired. Spuntare: ▪ **Deny:** In questo caso, il dispositivo negherà l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List. ▪ **Allow:** In questo caso, il dispositivo permetterà l'accesso alla rete a tutti i dispositivi consentendo l'accesso anche ai MAC non specificati.
Association Control	Spuntare **Association Control** per abilitare il modulo di filtraggio sui MAC dei soli dispositivi Wireless. Spuntare:

	▪ **Deny:** In questo caso, il dispositivo negherà l'accesso alla rete a tutti i dispositivi non specificatamente riportati nel campo MAC Address List. ▪ **Allow:** In questo caso, il dispositivo permetterà l'accesso alla rete a tutti i dispositivi consentendo l'accesso anche ai MAC non specificati.
ID/MAC/IP Address	E' possibile utilizzare questa sezione per assegnare un IP ad uno specifico MAC che fa richiesta DHCP.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.
Next	Cliccare per passare alla pagina seguente. Controllare la colonna ID.

Miscellaneous

Miscellaneous Items [HELP]

Item	Setting	Enable
Administrator Time-out	300 seconds (0 to disable)	
Remote Administrator Host : Port	/ :	☐
Discard PING from WAN side		☐
DoS Attack Detection		☐

Save Undo

Parametro	Descrizione
Administrator Time-Out	E' possibile inserire un tempo di idle prima del logout automatico dall'interfaccia di configurazione.
Remote Administrator Host/ Port	E' possibile limitare il controllo remoto ad un solo indirizzo IP, oppure lasciare 0.0.0.0 per permettere a tutti gli IP l'accesso. La sinttasi prevede: **IP/Subnet:porta**. E' inoltre possibile scegliere la porta di configurazione (LAN/WAN). Spuntare **enable** per abilitare il controllo remoto. E' opportuno creare una regola di Virtual Server permanente sull'IP lato LAN del Router e la porta impostata sul protocollo TCP.
Discard PING from WAN side	Spuntare per bloccare le risposte ai PING sulla WAN.
Dos Attack Detection	Spuntare per abilitare la modalità di controllori attacchi DoS (SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc).
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Vediamo nel dettaglio le tipologie di attacchi DoS:

- **Attacchi che mirano all'esaurimento della banda,** sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente può usare altri host che di fatto amplificano l'attacco.

- **Attacchi che mirano all'esaurimento delle risorse.**
- **Attacchi contro difetti di programmazione**, che mirano a sfruttare bug software o hardware.
- **Attacchi DoS generici.**

Segue una breve descrizione del funzionamento degli attacchi più comuni:

- **IP Spoofing:** è un attacco particolare in cui l'attaccante cerca di intromettersi in una connessione con lo scopo di abbatterla o di prenderne il controllo. Può essere fatto sia dall'interno della propria Lan (con possibilità più alte di successo se si dispone di LAN con HUB) che da Internet con possibilità di successo infinitamente inferiori. Grazie all' SPI il Router esamina a fondo i pacchetti che lo attraversano e confrontando molti parametri coi pacchetti precedenti della stessa connessione riesce a stabilire con efficacia se un pacchetto in arrivo è "spoofato" o meno.
- **Sync Flood:** come già accennato è un attacco che mira a esaurire le risorse del sistema che lo subisce. All'atto dell'instaurazione di una connessione viene spedito un pacchetto (dall'attaccante) col quale si avvisa che si vuole costruire la connessione. Il ricevente, cioè l'attaccato, alloca delle risorse e risponde con un pacchetto per proseguire la creazione della connessione. L'attaccato aspetta pazientemente il pacchetto di risposta (che non arriverà mai poiché l'attaccante avrà scelto o un IP di un host spento oppure starà attaccando l'host in questione impedendogli di rispondere). Le risorse allocate saranno bloccate sino a che non scade il timer associato. Nel frattempo l'attaccante ripeterà quest'attacco finendo col bloccare tutte le risorse disponibili nell'attaccato. Il firewall integrato nell' ADSL Router riconosce il tentativo di apertura di diverse connessioni provenienti dallo stesso IP e non allocherà le risorse. Certamente, a meno di trovarsi con sprovveduti, l'IP che verrà registrato nella tabella del sicurity logs non apparterrà all'attaccante.
- **Smurf Attack:** tenta invece di esaurire l'intera banda dell'host vittima, per fare questo può (a seconda della velocità della sua connessione) sfruttare anche delle sottoreti che fungono da amplificatore. Infatti l'indirizzo di broadcast di queste sottoreti vieni sfruttato e così tutti gli host di questa sottorete rispondono all'Echo Request richiesto dall'attaccante che avrà sostituito l'IP del mittente con quello dell'attaccato. All'attaccato tutti gli host risponderanno col pacchetto di Echo Reply generando un traffico intensissimo. Il Router filtra i pacchetti di Echo Reply in uscita trattandolo come un attacco.
- **Ping of Death:** quest'attacco particolare e dalle conseguenze variabili (anche a seconda del carico della macchina) viene generato creando un pacchetto ICMP di Echo Request fuori standard. Il pacchetto IP può infatti essere lungo, dalle spefiche RFC, al massimo 65536 bytes di cui 20 sono riservati per

l'header. Entro il Payload vengono inseriti i pacchetti di livello superiore, in questo caso l'ICMP (oppure TCP, UDP) che ha un header lungo 8 bytes. La lunghezza massima per il Payload del pacchetto ICMP è dunque 65535-20-8=60507 bytes. Sebbene un pacchetto del genere sia fuori specifica è comunque realizzabile, inoltre arriva frammentato alla destinazione (l'attaccato) dove verrà ricomposto (non verificandolo prima) ma a questo punto potrebbe generare un overflow dello stato di alcune variabili. Il firewall integrato si accorge di questo tipo di attacco e scarta il pacchetto in questione, aggiornando la tabella del security logs.

- **Land Attack:** sfrutta un errore presente in molti Sistemi operativi o Router che quando ricevono un particolare pacchetto (il cui IP di provenienza è uguale a quello di destinazione, cioè l'attaccato) di richiesta di connessione tentano di stabilirla ma vanno incontro ai più diversi blocchi. In pratica l'attaccato cerca di colloquiare con se stesso. Il Router elimina tutti i pacchetti con questa caratteristica.

3.5 Advanced Setting

Status

In questa sezione è possibile avere un quadro d'insieme dello stato di funzionamento dei moduli configurabili nel menu Advanced Setting.

System Time	[Modify]
Item	**Status**
System Time	Thu, 01 Jan 2009 18:58:27 +0000

Dynamic DNS	[Modify]
Item	**Status**
DDNS	Disable
Provider	-

Routing			[Modify]
Item	**Status**		
Dynamic Routing	Disable		
Static Routing	Disable		
Destination	Subnet Mask	Gateway	Hop

QoS				[Modify]
Item	**Status**			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time

Refresh

Parametro	Descrizione
Modify	Cliccare per modificare la sezione opportuna.
Refresh	Cliccare per aggiornare la pagina.

System Log

In questa sezione è possibile configurare il servizio Syslog integrato nel dispositivo e permettere l'invio di messaggi di stato al server Syslog o via mail.

System Log [HELP]

Item	Setting	Enable
IP address for syslogd		☐
Setting of Email alert		☐
• SMTP Server : port	:	
• SMTP Username		
• SMTP Password		
• E-mail addresses		
• E-mail subject		

Save Undo
View Log... Email Log Now

Parametro	Descrizione
IP Address of Syslog Server	Spuntare **Enable** ed insirire l'indirizzo LAN del server Syslog. Il dispositivo invierà continuamente i LOG di sistema.
Email Alert	Spuntare **Enable** per abilitare la funzionalità di invio mail di allerta. Cliccare (dopo aver configurato i parametri di invio) **Email Log Now** per testare la funzionalità di invio mail.
SMTP Server IP/Port	Digitare il nome o indirizzo IP del server SMTP. Digitare la porta usata per comunicare con il server SMTP. Solitamente la porta utilizzata è la 25. Ad esempio: **smtp.mail.out:25**
SMTP Username	Digitare la username.
SMTP Password	Digitare la password.
E-Mail addresses	Digitare l'indirizzo mail del destinatario. Sono supportati sino a 3 indirizzi separati dall'operatore ";" o ",".
E-Mail subject	Digitare il titolo della mail.
ViewLog	Cliccare

Save	Cliccare per salvare i settaggi inseriti.
Undo	Cliccare per cancellare quanto inserito e tornare alle condizioni iniziali.

Dynamic DNS

Tramite questa funzionalità è possibile registrare un dominio (del tipo nome dominio.dyndns.info) ed associarlo ad un IP dinamico. Ogni qual volta WebShare si riconnetterà od effettuerà un rinnovo dell'indirizzo IP associato all'interfaccia WAN, tramite il client incorporato, comunicherà al server Dynamic DNS il nuovo indirizzo IP assegnato dall'ISP. In questo modo, il Router ed i dispositivi ad esso collegati risulteranno sempre raggiungibili (se non per brevi periodi di fail legati al tempo di aggiornamento dell'associazione IP/dominio). Associando tale funzionalità con il Virtual Server è possibile:

- Gestire un server WEB interno alla propria LAN
- Attivare un server FTP pubblico sul quale depositare materiale da condividere
- Controllare in maniera remota una macchina od un dispositivo collegati al Router (es: IPCamera, NAS oppure direttamente un PC tramite apposito software)

Per poter usufruire di tutti i vantaggi del servizio DynDns è necessaria l'attivazione di un account sul sito www.dyndns.org (per maggiori informazioni, fare riferimento all'appendice relativa).
Una volta registrato il dominio DynDns, è possibile associarlo al Router tramite il client integrato come da procedura indicata di seguito:

Parametro	Descrizione
Dynamic DNS	Attiva o disattiva il client DynDNS integrato.
Provider	Indicare il provider di servizi DynDNS presso il quale si è precedentemente registrato un account DynDNS. I provider supportati sono: **Dynamic DNS**, **No-IP.com**, **TZO.com** e **dhs.org.** Per accedere al sito d effettuare la registrazione,

	cliccare **Provider WebSite.**
HostName	Inserire il dominio registrato presso il provider di servizi DDNS.
Username/Email	Inserire il nome utente utilizzato in fase di registrazione dell’account DDNS.
Password	Inserire la password utilizzata in fase di registrazione dell’account DDNS.
Save	Cliccare per salvare i settaggi inseriti.
Undo	Cliccare per cancellare quanto inserito e tornare alle condizioni iniziali.

A questo punto WebShare è sempre e comunque raggiungibile dall’esterno. E’ possibile ad esmpio ospitare un sito WEB o FTP (ruotando le opportune porte).
In questo modo ogni utente esterno interrogherà il server DDNS che gli restituirà di volta in volta l’indirizzo IP assegnato dall’ISP al WebShare.

	Il client integrato eseguirà la procedura di sincronizzazione col server ad ogni riconnessione del profilo PPP. Si consiglia quindi di non utilizzare questa funzionalità in accordo con linee particolarmente rumorose che potrebbero provocare eccessive richieste di sincronizzazione, con conseguente disattivazione dell’account.

	Per maggiori dettagli consultare l’Appendice B.

QoS

Il dispositivo per eccellenza nella LAN in cui si attua la multiplazione statistica delle risorse è indubbiamente l'apparato responsabile della connettività, nel caso in esame l'Adsl2+ Router. In effetti il Router ADSL permette, indipendentemente dalla tipologia di contratto fornita dall'ISP, ad una moltitudine di PC di condividere la singola connessione ADSL. Generalmente questa situazione rappresenta spesso un collo di bottiglia, in quanto ciascun PC vorrebbe poter utilizzare il massimo della connettività offerta dal Router che invece deve permettere, sempre e comunque, agli altri utenti di accedere alla risorsa.
In una LAN tradizionale non esiste un altro dispositivo responsabile della gestione di una così marcata multiplazione. L'accesso dati verso un server centralizzato, nel caso di rete correttamente strutturata con dorsale in gigabit, non rappresenta solitamente un problema visto il corretto dimensionamento delle risorse (10 accessi contemporanei a piena banda in F/E non sarebbero sufficienti a saturare questo collegamento).
Nel caso del Router ADSL purtroppo il limite è fornito dalla velocità della connessione ADSL spesso limitata ad una frazione di megabit. In questo megabit, dozzine di utenti, devono poter effettuare Navigazione WEB, Accesso/Invio della propria posta, effettuare download, servizi di streaming e così via.
Il risultato complessivo genera solitamente un accumulo di richieste inviate verso il Router e da questo bufferizzate in attesa di essere processate non appena le risorse siano nuovamente disponibili. La logica utilizzata dal Router è solitamente di tipo FIFO. In questo scenario, tipico già nella piccola azienda, abbiamo un'enorme crescita dei tempi di latenza che generano:

- Attesa via via crescenti
- Impossibilità nell'uso di servizi in tempo reale (VoIP, Streaming, Netmeeting)
- Scadere di taluni Timeout
- Lo scadere di un Timeout genera la ritrasmissione di interi pacchetti, ciò produce un enorme spreco di risorse avvicinando così la rete verso la congestione.

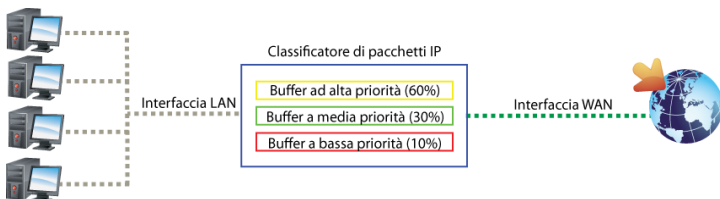
Il Router ADSL permette di risolvere/limitare questo problema cambiando radicalmente la politica utilizzata nel processare i pacchetti IP inviatigli. Ogni pacchetto ricevuto dal Router viene anzitutto classificato, in base a criteri specificati dall'amministratore, e quindi memorizzato, laddove non ci siano le risorse disponibili, in un buffer opportuno. Il dispositivo permette per ogni servizio/applicazione:

- di garantire una percentuale minima di banda
- limitare un massimo di banda

questo tanto in upload che download.

Il Router dunque non processa più con logiga FIFO il buffer dei pacchetti ma prima classifica il pacchetto, in base alle policy, e poi assegna le risorse disponibili.
I vantaggi derivanti dall'uso di attente politiche di Priorità sono:

- Attesa media contenuta
- Riduzione di overhead di ritrasmissione
- Piena fruibilità di servizi quali VoIP, Netmeeting, Streamin e così via.

Questo da una parte genera un più razionale utilizzo della risorsa comune e rende meno probabili le condizioni che portano alla saturazione della rete.
Nella figura sottostante è possibile vedere il diagramma a blocchi del dispositivo.

	Resta inteso che dare ad ogni servizio/IP priorità massima, significa di fatto accorpare gran parte del traffico in un solo buffer che viene comunque processato con logica FIFO. Questo non porta a nessun risultato apprezzabile.

QoS Rule

Item	Setting
QoS Control	Enable
Bandwidth of Upstream	kbps (Kilobits per second)

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use rule#
1	:	:	High		(0) Always
2	:	:	High		(0) Always
3	:	:	High		(0) Always
4	:	:	High		(0) Always
5	:	:	High		(0) Always
6	:	:	High		(0) Always
7	:	:	High		(0) Always
8	:	:	High		(0) Always

Save Undo

Parametro	Descrizione
QoS Control	Spuntare per attivare la funzionalità QoS.
Bandwith of Upstream	Indicare in Kbps la banda in upload.
Local IP:Port	Inserire l'indirizzo IP e la porta di provenienza.
Remote IP: Port	Inserire l'indirizzo IP e la porta di destinazione.
QoS Priority	Selezionare la tipologia di criticità nella combo Box. Sono disponibili 3 livelli **High, Low, Normal.** ▪ **High:** il dispositivo alloca a questa tipologia di traffico il 60% della banda disponibile. ▪ **Normal:** il dispositivo alloca a questa tipologia di traffico il 30% della banda disponibile. ▪ **Low:** il dispositivo alloca a questa tipologia di traffico il 10% della banda disponibile.
Enable	Spuntare per abilitare la regola creata.
Use Rule#	Selezionare una schedulazione per la regola.

Save	Cliccare per salvare i settaggi inseriti.
Undo	Cliccare per cancellare quanto inserito e tornare alle condizioni iniziali.

	Tutto il traffico non specificatamente assegnato ai buffer High/Low verrà classificato come Normal

SNMP

L’SNMP (Simple Network Management Protocol) è un protocollo che viene utilizzato per il management ed il controllo del network. E’ richiesto un software apposito in un PC della LAN Il protocollo SNMP può funzionare indifferentemente su IP, IPX o Apple Talk. Differenti oggetti creano una struttura SNMP (Agenti SNMP, Network Management Stations[NMS], Network Management Protocols ed Management Information Base[MIB].
Un agente SNMP risiede tipicamente in un device intelligente della rete e viene configurato e controllato da un NMS tramite messaggi SNMP. In ogni MIB è contenuto un identificatore OID dell’agente. Le TRAP vengono inviate verso l’IP dell’NMS utilizzando specifiche porte e sono utilizzate per segnalare particolari eventi.
SNMP Access Control (E’ richiesto un software apposito in un PC della LAN) – Simple Network Management Protocol.

- Read Community: Specificare il nome per identificare la Read Community (e l’indirizzo IP da cui si può accedere). E’ una sorta di password che il dispositivo controlla prima di concedere l’acesso in lettura dei dati.
- Write Community: Specificare il nome per identificare la Write Community (e l’indirizzo IP da cui si può accedere). E’ una sorta di password che il dispositivo verifica prima di poter accedere alla configurazione.
- Trap Community: Specificare un nome per identificare una Trap Community e un indirizzo IP cui verrano inviate le Trap.

SNMP: SNMPv2c

L’SNMPv2c include le caratteristiche avanzate del protocollo SNMPv2, esclusa la sicurezza che è rimasta quella del protocollo SNMPv1.
SNMPv3 (non supportato dal WebShare 142WN) include inoltre un robusto meccanismo di autenticazione per la configurazione remota.

SNMP Setting [HELP]

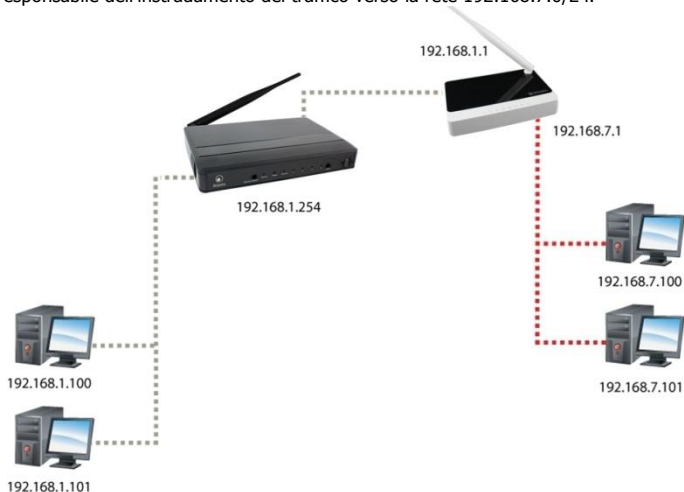
Item	Setting
Enable SNMP	☐ Local ☐ Remote
Get Community	
Set Community	
IP 1	
IP 2	
IP 3	
IP 4	
SNMP Version	◉ V1 ○ V2c
WAN Access IP Address	

Save Undo

Parametro	Descrizione
Eanble SNMP	Spuntare **Local** per autorizzare solo la LAN, **Remote** per autorizzare la WAN. Spuntarli entrambi per permettere un accesso sia locale che remoto.
Get Community	Specificare il nome per identificare la Read Community. E' una sorta di password che il dispositivo controlla prima di concedere l'acesso in lettura dei dati.
Set Community	Specificare il nome per identificare la Write Community. E' una sorta di password che il dispositivo verifica prima di poter accedere alla configurazione.
IP 1/2/3/4	Digitare l'indirizzo IP delle macchine dove risiede il client SNMP ed a cui vengono inviati i messaggi di TRAP.
SNMP Version	Spuntare la versione del protocollo da utilizzare. Sono disponibili V1 o V2c.
WAN Access IP Address	Serve per limitare l'accesso da WAN ad un determinato IP.
Save	Cliccare per salvare i settaggi inseriti.
Undo	Cliccare per cancellare quanto inserito e tornare alle condizioni iniziali.

	La porta/protocollo utilizzata dall’SNMP è la 161 in UDP.

Routing

Permette di configurare gli instradamenti statici (sino a d 8) nel caso in cui sia necessario effettuare routing all'interno della rete LAN.
Per comprendere al meglio questa funzionalità, ci serviremo di un esempio.
Si ponga di avere 2 segmenti di rete (192.168.1.0/24 ed 192.168.7.0/24), dove il dispositivo con indirizzo 192.168.1.1 appartente alla LAN del Router sia il responsabile dell'instradamento del traffico verso la rete 192.168.7.0/24.

Per poter raggiungere i client posti sulla sottorete 192.168.7.0/24, sarà necessario creare una regola di instradamento statico come segue:

Parametro	Descrizione
Destination	Indicare il segmento di rete o l'indirizzo IP da raggiungere.
Netmask	Indicare la maschera di rete relativa all'indirizzo dichiarato nel campo Destination.
Gateway	Inserire l'IP della macchina responsabile dell'instradamento dei pacchetti verso il segmento di rete da raggiungere.
HOP	Introdurre il costo in HOP. Usualmente tale valore è 1. Mettere tale valore in funzione del numero di Router che è necessario attraversare per arrivare alla rete desiderata.
Enable	Spuntare per abilitare l'instradamento statico.

Premere su **Save** per aggiungere la regola di instradamento alla tabella di instradamento del Router.

System Time

Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente. E' possibile utilizzare una delle 3 modalità seguenti:

- **Get Date and Time by NTP Protocol:** Selezionare per utilizzare un server NTP da cui ricevere le impostazioni di data/ora. Selezionare nel campo **Time Server** l'indirizzo IP del server o il suo nome. Selezionare poi in **Time Zone** il fuso orario di appartenenza. Cliccare poi su Sync Now per effettuare la sincronizzazione.
- **Set Date and Time using PC's Date and Time:** Selezionare per utilizzare come impostazioni per data/ora quele del PC da cui si sta effettuando il management.

System Time [HELP]

Item	Setting
Time Zone	* Not yet configured! The default is GMT+00:00
Auto-Synchronization	Enable Time Server (RFC-868): Auto

Save | Undo

Sync with Time Server

Sync with my PC (Monday December 20, 2010 17:44:56)

Parametro	Descrizione
Time Zone	Selezionare nella Combo-Box il fuso orario di appartenenza.
System Time	Viene visualizzata l'ora e la data del dispositivo.
Get Date and Time by NTP Protocol:	Selezionare per utilizzare un server NTP da cui ricevere le impostazioni di data/ora. Selezionare nel campo **Time Server** l'indirizzo IP del server o il suo nome. Selezionare poi in **Time Zone** il fuso orario di appartenenza. Cliccare poi su **Sync Now** per effettuare la sincronizzazione.
Sync with my PC	Selezionare per utilizzare come impostazioni per data/ora quele del PC da cui si sta effettuando il management.
Save	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Il protocollo di default, l'NTP (RFC 1305), è simile al protocollo dell'ora (RFC 868). Il formato dell'ora(RFC 868) visualizza un numero intero 4-byte che dà il numero totale di secondi dal

	1970/1/1 a 0:0:0. E’ possibile utilizzare il seguente server **NTP: 128.138.140.44**

	Verificare che il Router abbia i DNS (altrimenti non potrà risolvere i nomi dei server NTP e quindi ottenere le informazioni orarie/data).

Schedule Rule

La funzionalità Time Schedule/Schedule Rule consente di impostare fino a 8 TimeSlot che aiuteranno l'utente a gestire nel miglior modo la sezione Firewall, Virtual Server e Wireless. E' possibile impostare i giorni e gli orari in cui le diverse regole di firewalling, virtual server sono attive. Questa funzionalità è strettamente correlata alla sincronizzazione dell'orologio di sistema configurabile all'interfaccia **System Time**.

Schedule Rule [HELP]

Item	Setting
Schedule	Enable

Rule#	Rule Name	Action
1		New Add
2		New Add
3		New Add
4		New Add
5		New Add
6		New Add
7		New Add
8		New Add
9		New Add
10		New Add

<<Previous | Next>> | Save | Add New Rule...

Parametro	Descrizione
Schedule	Spuntare **Enable** per attivare tale funzionalità.
Edit	Per cambiare un timeslot.
Delete	Per rimuovere un timeslot.
Save	Cliccare per salvare le impostazioni inserite.
Add New Rules	Cliccare per aggiungere un nuovo Time Slot (rule).

Schedule Rule Setting [HELP]

Item	Setting
Name of Rule 1	
Policy	Inactivate except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Save Undo Back

Parametro	Descrizione
Name of Schedule	Digitare il nome del TimeSLot.
Week Day	E' possibile definire un orario di inizio (hh:mm) e di fine (hh:mm) indipendente per ogni giorno della settimana o comune (in questo caso scrivere le informazioni orarie in **Every Day**).
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.
Back	Cliccare per tornare alla schermata precedente.

3.6 NAS

Disk Utility

In questa sezione è possibile vedere lo stato della periferica di memorizzazione connessa.
Quando nessuna periferica è collegate verrà mostrata l'immagine di sotto (il LED STATUS è lampeggiante).

	Si raccomanda, soprattutto se la periferica di memorizzazione è già formattata, di attendere qualche minuto per l'analisi. Questo tempo è funzione della dimensione della periferica di Storage. Quando si inserisce una periferica questa viene sottoposta al processo di Check. Questo terminerà quando il LED STATUS diverrà acceso fisso.

Una volta finita la fase di analisi (check), che potrebbe durare qualche minuto, verrà mostrata l'immagine di sotto.

Disk Distribution

Disk Total Capacity = 7948 MB

Partition	Free(MB)	Used(MB)	Total(MB)
1 [EXT3]	5501	1959	7460

*Warning! Formatting will erase all data on this partition.

Format Check

Parametro	Descrizione
Partition	Viene mostrata la tipologia di File System rilevata sulla periferica di memorizzazione.
Free(MB)	Viene mostrato, in MB, lo spazio inutilizzato nella periferica di memorizzazione.
Used(MB)	Viene mostrato, in MB, lo spazio utilizzato nella periferica di memorizzazione.
Format	Cliccare per far partire il processo di formattazione. Ogni dato contenuto nella periferica verrà irrimediabilmente perso. Durante questa fase il dispositivo può essere non raggiungibile. Attendere che il LED Status diventi fisso.

Check	Cliccare per effettuare un’analisi della periferica di memorizzazione. Questo processo aiuta a risolvere tutta una serie di problematiche (analisi partizioni, spazio libero, files memorizzati). Lo stato di avanzamento del processo verrà mostrato tramite una barra di stato. Il processo potrebbe richiedere qualche minuto.

	WebShare 242WN supporta i seguenti formati: • **FAT16:** lettura e scrittura • **FAT32:** lettura e scrittura • **EXT2:** lettura e scrittura • **NTFS:** sola lettura

File Sharing

In questa sezione è possibile impostare le configurazioni riguardanti Samba ed FTP.

File Sharing

Item	Setting
Computer Name	NAS
WorkGroup	WORKGROUP
Server Comment	samba server
	Save / Undo / FTP Service Configuration

Parametro	Descrizione
Computer Name	Digitare il nome del dispositivo. Verrà mostrato in Windows
WorkGroup	Digitare il nome del workgroup dove il dispositivo è collocato. E' importante sia identico a quello utilizzato dal PC da cui si vuole accedere.
Server Comment	Digitare una descrizione utile al riconoscimento del dispositivo.
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.
FTP Service Configuration	Cliccare per accedere alla configurazione del servizio FTP.

FTP Setting

Item	Setting
FTP	Enable / Disable
FTP Port	21
FTP Max Connection per IP	2
FTP MAX Clients	5
Client Support UTF8	Yes / No
Codepage	Latinl+ Europe(CP850)
	Save / Undo

Parametro	Descrizione
FTP	Spuntare **Enable** per abilitare il servizio.
FTP Port	Digitare la porta utilizzata dal protocollo FTP. Normalmente la porta è la 21.
FTP Max Connection per IP	Scegliere tramite la combo-box il numero massimo di connessioni per IP ammesse. I valori permessi vanno da 2 a 5.
FTP Max Clients	Scegliere tramite la combo-box il numero massimo di connessioni FTP ammesse. I valori permessi vanno da 1 a 20.
Client Support UTF8	Utilizzare se è supportato dal client FTP in uso. Si rimanda alla manualistica di quest'ultimo.
CodePage	Scegliere tramite la combo-box quello più adatta al proprio utilizzo.
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.

Access Control

In questa sezione è possibile impostare la modalità di accesso riguardanti Samba ed FTP.

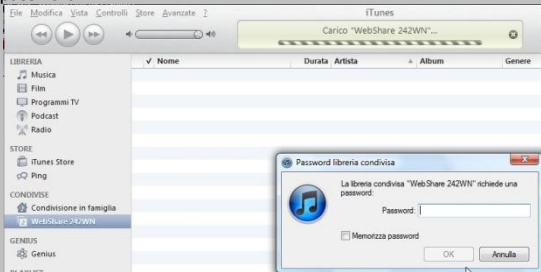
Parametro	Descrizione
Security level	Normalmente il dispositivo permette un accesso (FTP/Samba) in modalità Guest. Per autorizzare solo un accesso con password spuntare **Authorization Mode.**
Save	Cliccare per salvare le impostazioni inserite.
User Configuration	Cliccare per accedere alla configurazione dei profili utenti. Questo forza il dispositivo a funzionare in **Authorization Mode.**

User Access Configuration

Item	Setting
User Name	(Max. 20 users)
Password	

ID	Username	Password	Select

Add | Delete | Cancel | Back

Parametro	Descrizione
Username	Digitare la username dell'account.
Password	Digitare la password dell'account.
Add	Cliccare per creare l'account impostato.
Delete	Spuntare nel campo select l'account da eliminare. Premere Delete per rimuoverlo dal sistema.
Cancel	Cliccare per salvare le impostazioni inserite.
Back	Cliccare per tornare alla schermata precedente.

WebShare 242WN supporta un massimo di 20 profili utente.

iTunes Server

WebShare, una volta attivato il server iTunes®, diviene a tutti gli effetti un media-server in grado di inviare in streaming musica, video o altri contenuti digitali direttamente agli apparati riproduttori (quali Ipod).

iTunes Server Configuration

Item	Setting
Service	○ Enable ◉ Disable
Service Name	
Service Port	3689
Access Password	
	Save Undo

Parametro	Descrizione
Service	Spuntare **Enable** per abilitare il servizio.
Service Name	Digitare il nome dato al server iTunes. Questo verrà mostrato in iTunes. E' opportuno differenziarlo da altri presenti nella stesa rete.
Service Port	Scegliere la porta utilizzata. Normalmente la porta utilizzata è la 3689.
Access Password	digitare una password nel caso si volesse limitare gli accessi. Se tale campo è lasciato vuota iTunes accederà senza problemi. Nella figura è mostrata la schermata in cui viene richiesta la password.
Save	Cliccare per salvare le impostazioni inserite.

Undo	Cliccare per cancellare le impostazioni inserite.

	Quando il servizio iTunes è attivo nel WebShare è possible salvare i file MP3 nella cartella indicata in **Shared Folders(Condivisione)** ed effettuarne il playback direttamente da WebShare r che verrà visualizzato in iTunes sotto **Shared Devices(Condivisione).**

	Alcune tipologie di file potrebbero non essere pienamente supportate. Non è un problema del prodotto.

	L'intervallo di rescan (indica i secondi passati i quali il sistema controllerà nelle cartelle condivise la presenza di nuovi files) di default è 120s. Le tipologie di file supportate dal server iTunes sono: • .mp3 • .aac • .m4a • .m4p

	Per accedere alla configurazione dettagliata del server iTunes digitare nel browser: **IP Router:porta** e utilizzare le credenziali di accesso preimpostate (admin, atlantis).

	Il Server iTunes leggerà tutti e soli i file nella cartella **Download**.

Download Assistant (FTP)

In questa sezione è possibile utilizzare i servizi di download schedulato o BitTorrent.

Download Assistant - FTP

Item	Setting
Download Type	◉ FTP ○ HTTP ○ BT
Job Name	
URL	Port 21
Save To	/C/Downloads/FTP
Login method	◉ Anonymous ○ Account
Username	
Password	
Start Time	○ Schedule ◉ At Once
Time	2010 / Dec / 21 - 14 : 11

*When you use the download service of FTP, HTTP, or BT, please check if these files you downloaded are legal or not.

E-mail Alert Configuration | Save | Undo

Parametro	Descrizione
Download Type	Spuntare **FTP.**
Job Name	Digitare il nome dato al processo creato.
URL	Digitare il percorso da cui effettuare il download utilizzando in protocollo FTP (**IP/percorso/File**). Digitare poi la porta richiesta dal server cui si desidera connettersi. Normalmente è la porta 21. Non è necessario aggiungere il prefisso **ftp://**
Save To	Digitare il percorso dove il file scaricarto verrà salvato. Usualmente è: **/C/download/FTP**
Login Method	Spuntare **Anonymous** se il server FTP non richiede autenticazione. Selezionare **Account** nel caso in cui il server FTP richieda autenticazione.
Username/ Password	Digitare username e password richieste dal server FTP.

Start Time	Selezionare **At Once** per effettuare il download una volta soltanto, oppure spuntare **Schedule** per impostare una programmazione temporale.
Time	Selezionare la data di inizio partenza del Job programmato.
E-mail Alert Configuration	Cliccare per configurare il servizio di invio mail quando il downbload è terminato.
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.

Per controllare i JOB schedulati accedere a **NAS->Download Status** e selezionare **Scheduled** nella combo box **View**.

L'utilizzo di servizi di download sono regolari se i file scaricati non sono protetti da diritti d'autore. **Atlantis non può essere ritenuta responsabile in caso di download di materiale protetto da diritti d'autore. L'utilizzatore fa questo a suo rischio e pericolo.**

E-mail Alert Configuration

Item	Setting
HTTP download alert	Enable Disalbe
FTP download alert	Enable Disalbe
BT download alert	Enable Disalbe
USB download alert	Enable Disalbe
SMTP Server Address	
SMTP Server Port	
SMTP User Name	
SMTP Password	
Email Address	
Email Subject	
Reservation Disk space	0 MB

Back Save Undo Test E-mail

Parametro	Descrizione
http/FTP/BT/USB Download Alert	Spuntare per l'invio di una mail quando un job è terminato.
SMTP Server Address	Digitare il nome o indirizzo IP del server SMTP.
SMTP Server Port	Digitare la porta usata per comunicare con il server SMTP. Solitamente la porta utilizzata è la 25.
SMTP Username	Digitare la username.
SMTP Password	Digitare la password.
EMail address	Digitare l'indirizzo mail del destinatario.
EMail Subject	Digitare il titolo della mail. Sino a 64 caratteri.
Reservation Disk Space	Digitare in MB lo spazio riservato. Il sistema invierà una mail quando il limità verrà raggiunto.
Back	Cliccare per tornare alla pagina precedente.
Undo	Cliccare per tornare ai valori preimpostati nella maschera.

Save	Cliccare per salvare i settaggi impostati.
Test E-Mail	Cliccare per testare il tutto con l’invio di una mail di prova.

Download Assistant (HTTP)

In questa sezione è possibile utilizzare i servizi di download schedulato http.

Download Assistant - HTTP

Item	Setting
Download Type	FTP HTTP BT
Job Name	
URL	
Save To	/C/Downloads/HTTP
Start Time	Schedule At Once
Time	2010 / Dec / 21 - 14 : 56

*When you use the download service of FTP, HTTP, or BT, please check if these files you downloaded are legal or not.

E-mail Alert Configuration | Save | Undo

Parametro	Descrizione
Download Type	Spuntare **HTTP.**
Job Name	Digitare il nome dato al processo creato.
URL	Digitare il percorso da cui effettuare il download utilizzando in protocollo HTTP. (**IP/percorso/File**). Non è necessario aggiungere il prefisso **http://**
Save To	Digitare il percorso dove il file scaricarto verrà salvato. Usualmente è: **/C/download/HTTP**
Start Time	Selezionare **At Once** per effettuare il download una volta soltanto, oppure spuntare **Schedule** per impostare una programmazione temporale.
Time	Selezionare la data di inizio partenza del Job programmato.
E-mail Alert Configuration	SI veda la sezione precedente (**Download Assistant (HTTP)**).
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.

Per controllare i JOB schedulati accedere a **NAS->Download Status** e selezionare **Scheduled** nella combo box **View**.

L'utilizzo di servizi di download sono regolari se i file scaricati non sono protetti da diritti d'autore. **Atlantis non può essere ritenuta responsabile in caso di download di materiale protetto da diritti d'autore. L'utilizzatore fa questo a suo rischio e pericolo.**

Download Assistant (BT)

In questa sezione è possibile utilizzare il client BitTorrent integrato per scaricare da internet direttamente sulla periferica di memorizzazione connessa alla porta USB a PC scpento.

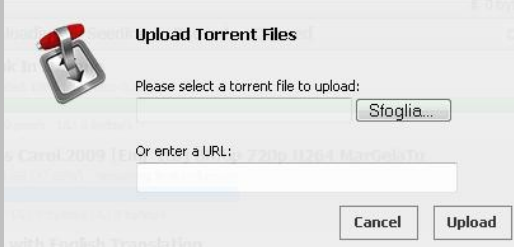
Download Assistant - BitTorrent

Item	Setting
Download Type	FTP HTTP BT

Open Remove Pause Resume Pause All Resume All Filter Inspector

3 Transfers 0 bytes/s 0 bytes/s

All Downloading Seeding Paused Queued Filter

1000 E-Book In Italiano
376.7 MB, uploaded 108.6 MB (Ratio 0.29)
Seeding to 0 of 0 peers - UL: 0 bytes/s

A Christmas Carol.2009 [Eng_Ita] BRRip 720p H264 MarGelaTu
746.0 MB of 1.55 GB (47.05%) - remaining time unknown
DL 0 of 0 peers - DL: 0 bytes/s UL: 0 bytes/s

Holy Quran with English Translation
682.4 MB, uploaded 13.5 MB (Ratio 0.02)
Seeding to 0 of 0 peers - UL: 0 bytes/s

Parametro	Descrizione
Download Type	Spuntare **BT.**
Open	Cliccare per accedere alla finesra di immissione del torrent.

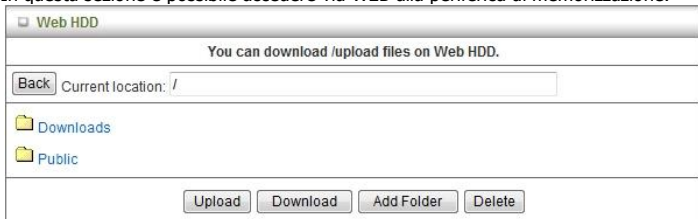
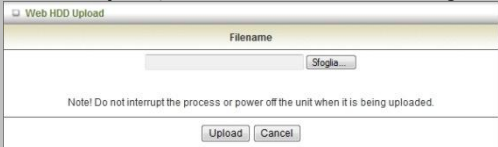
	Verrà visualizzata la finestra sotto riportata. ▪ **URL:** Inserire l'url da scaricare ▪ Cliccare su **Browse** ed indicare il file di Torrent scaricato e cliccare poi su **Upload.** ▪ **URL:** Inserire l'**url** da scaricare e cliccare poi su **Upload.**
Remove/ Pause/ Resume	Selezionare un task, questo verrà evidenziato dallo sfondo di colore blu, e cliccare il bottone per attivare la funzione richiesta.
Pause ALL/ Resume ALL	Mette in pausa/riattiva tutti i task.
Filter	E' possibile filtrare (selezionando ALL, Downloading, Seeding, Paused, Queued) i task mostrati. Cliccare su **Filter** e cliccare poi sulla tipologia desiderata.
Inspector	Selezionare un task, questo verrà evidenziato dallo sfondo di colore blu, e cliccare il bottone **Inspector** per visualizzare maggiori dettagli sul task.
	Cliccare sul bottone e poi su preferences. Verrà visualizzata la schermata seguente:

	Preferences Add transfers: Download to: /var/usb/C/Downloads/BT/downloads Start transfers when added Network: Incoming TCP Port: 51413 Web Client: Refresh Rate: 5 seconds Cancel Save ▪ **Download To:** Digitare il percorso dove il file scaricarto verrà salvato. Usualmente è: **/C/download/BT/Downloads** ▪ **Start Transfer when added:** spuntare per far partire un nuovo task una volta aggiunto. ▪ **Incoming Port:** digitare la porta utilizzata. ▪ **Web Cliebt Refresh:** digitare in secondi l'intervallo di refresh. Più basso è tale valore più vengono drenate risorse. ▪ **Cancel:** Cliccare per cancellare. ▪ **Save:** Cliccare per salvare le impostazioni inserite.
⬇ 300.0 KB/s ⬆ 0 bytes/s	Viene visualizzata la velocità in download/upload del modulo Torrent.

	L'utilizzo di servizi di download sono regolari se i file scaricati non sono protetti da diritti d'autore. **Atlantis non può essere ritenuta responsabile in caso di download di materiale protetto da diritti d'autore. L'utilizzatore fa questo a suo rischio e pericolo.**

	Il sistema supporta 3 task contemporanei, tutti i vari task ulteriori saranno accodati ed eseguiti quando i task attivi verranno esauriti/rimossi.

Download Status

In questa sezione è possibile vdere lo stato dei vari task FTP/HTTP.

Parametro	Descrizione
View	Selezionare **Running/Scheduled/Waiting.**
Pause	Selezionare un task e cliccare **Pause** per metterlo in pausa.
Delete	Selezionare un task e cliccare **Delete** per rimuoverlo dal sistema.
Resume	Selezionare un task e cliccare **Resume** per forzarne la ripartenza immediata.
Start Now	Selezionare un task e cliccare **Start Now** per forzarne la partenza immediata.
Refresh	Cliccare per aggiornare le informazioni a video.
E-mail Alert Configuration	SI veda la sezione precedente (**Download Assistant (HTTP)**).
Save	Cliccare per salvare le impostazioni inserite.
Undo	Cliccare per cancellare le impostazioni inserite.

Web HDD

In questa sezione è possibile accedere via WEB alla periferica di memorizzazione.

Parametro	Descrizione
Upload	Permette l'upload di file nelle cartelle del sistema. Cliccare su **Upload**, verrà visualizzata la schermata seguente. Cliccare su **Sfoglia** per selezionare il file da caricare e cliccare su **Upload.**
Download	Permette, una volta scelto un file, lo scaricamento sul proprio PC.
Add Folder	Cliccare per creare una cartelle. Immetere il nome e cliccare su **Create.**
Delete	Selezionare un file/cartella e cliccare per rimuoverla dal sistema.

3.7 ToolBox

System Info

System Log

Item	Info
WAN Type	PPP over ATM (R0.27a1(beta01))
Display time	Mon Jun 01 02:17:09 2009

Time	Log
domenica 31 maggio 2009 23.59.11	Admin from 192.168.1.45 login successfully
lunedì 1 giugno 2009 0.00.50	Admin from 192.168.1.45 logged out
lunedì 1 giugno 2009 0.02.14	Admin from 192.168.1.45 login successfully
lunedì 1 giugno 2009 1.19.40	Admin from 192.168.1.45 login successfully
lunedì 1 giugno 2009 1.52.22	Admin from 192.168.1.45 login successfully
lunedì 1 giugno 2009 2.14.53	Admin from 192.168.1.45 login successfully

Refresh | Download | Clear logs

Parametro	Descrizione
WAN Type	Viene mostrata la tipologia di interfaccia WAN (3G, ADSL).
Display Time	Viene mostrata l'ora/data del dispositivo.
Time	Viene mostrata l'ora/data del log.
Log	Viene mostrata una descrizione dell'evento registrato.
Refresh	Cliccare per aggiornare i log visualizzati a video.
Download	Cliccare per salvare su PC (in formato LOG) i file di LOG di sistema.
Clear Logs	Cliccare per svuotare la memoria di Logs del sistema.

Firmware Upgrade

Per effettuare l'upgrade del firmware del dispositivo è necessario anzitutto scaricare dal sito **www.atlantis-land.com** (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto alla voce **Firmware Upgrade** e premere poi il tasto **Browse** ed indicare la path contenente il firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. E' opportuno staccare, durante la fase di upgrade, la linea ADSL dal dispositivo.
Durante la fase di upgrade il Router indicherà lo stato di completamento della riscrittura del firmware mostrando un indicatore percentuale.

<table>
<tr>
<td>
</td>
<td>

E' opportuno garantire, durante l'intera fase di upgrade, al Router ADSL l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.
Staccare il cavo RJ11 dal Router e verificare che solo un cavo ethernet sia connesso (quello del PC da cui si effettua l'upgrade).
Effettuare l'upgrade utilizzando una connessione wired e non wireless. Questo potrebbe danneggiare il dispositivo ed invalidare così la garanzia.
Non utilizzare file di restore generati con versioni anteriori di firmware. Questo potrebbe rendere instabile il dispositivo.
Durante la procedura di upgrade è opportuno non chiudere il browser Web, caricare nuove pagine o cliccare su link. Questo potrebbe danneggiare il firmware e rendere inusabile il dispositivo.

</td>
</tr>
</table>

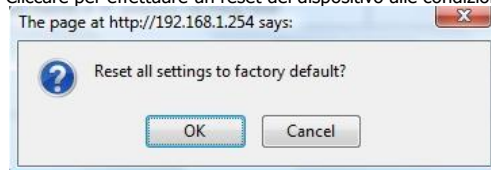
Backup Setting

Il WebShare Router consente di effettuare un backup (ripristino) sul (dal) disco fisso del PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.
Per effettuare il Backup cliccare sul bottone **Backup Setting**. Non resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file con estensione BIN).
Per effettuare il **Ripristino** accedere alla sezione **Firmware Upgrade**, indicando il percorso (**Browse**) dove è contenuto il file contenente la configurazione e cliccare poi su **Upgrade.**
La procedura è piuttosto lenta (il tempo complessivo può superare i 2 minuti) e termina con il riavvio del dispositivo.

	Non editare per nessuna ragione il file di backup, questo potrebbe bloccare e rendere inutilizzabile il dispositivo.

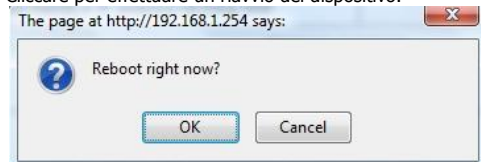
	Non utilizzare file di Backup provenienti da versioni di firmware differenti.

Reset to Default

Cliccare per effettuare un reset del dispositivo alle condizioni iniziali.

Cliccare su **OK** per conferma.

	Dopo che il dispositivo è acceso, effettuare per effettuare il reset la seguente procedura: Premere **Wireless ON/OFF** e **WPS** per circa 5 secondi. Il LED Status si spegnerà, per indicare l'avvenuto reset dell'apparato.

Reboot

Cliccare per effettuare un riavvio del dispositivo.

Cliccare su **OK** per conferma.

Miscellaneous

Miscellaneous Items [HELP]

Item	Setting
MAC Address for Wake-on-LAN	Wake up
Domain Name or IP address for Ping Test	Ping
Save Undo	

Parametro	Descrizione
Mac Address for Wake-on-LAN	Questa funzionalità permette di "risvegliare" un PC collegato via cavo al Router mediante la generazione di un apposito pacchetto (detto pacchetto di WakeUp) instradato a livello MAC dal Router alla scheda di rete del PC da risvegliare. E' necessario inserire il MAC address (con la sintassi: 00-11-22-33-44-FF) della macchina di cui si vuole effettuare il Wake-on-LAN. Cliccare su **Wake-UP** per inviare il pacchetto di wake-up al MAC inserito.
Domain Name or IP address for Ping Test	Inserendo un nome o indirizzo IP è possibile inviare un pacchetto di PING e vedere se il sito risponde. Cliccare **Ping** per inviare il pacchetto.
Save	Cliccare per salvare i settaggi inseriti.
Undo	Cliccare per cancellare quanto inserito e tornare alle condizioni iniziali.

	Per maggiori dettagli sul Wake-on-LAN si consulti il capitolo 5.

5. Risoluzione dei problemi

Questo capitolo illustra come identificare e risolvere eventuali problemi sul WebShare Torrent 242 WN .

A.1 Utilizzare i LED per la diagnosi dei problemi

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED STATUS non si accende

Steps	Azione Correttiva
1	Accertarsi che l'alimentatore sia connesso al WebShare Router e alla rete elettrica. Utilizzare unicamente l'alimentatore fornito a corredo (9V, AC-DC).
2	Verificare che l'alimentatore sia connesso a una presa elettrica attiva e in grado di fornire la tensione necessaria al funzionamento del prodotto.
3	Accertarsi che il Plug dell'alimentatore sia correttamente inserito.
4	Accertarsi che il bottone di accensione, posto sul frontalino, sia su ON.
5	Se il problema persiste contattare l'assistenza tecnica Atlantis.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra il router e il PC o lo Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis.

A.1.3 LED WAN

Il LED WAN non si accende.

Steps	Azione Correttiva
1	Verificare che il cavo telefonico e la presa a muro funzionino correttamente.
2	Verificare che il Provider abbia attivato il servizio ADSL.
3	Accedere al dispositivo in **Status->ADSL MODEM STATUS** e controllare il valore **SNR Margin in downstream**.

4	Se il problema persiste contattare l'assistenza tecnica Atlantis.

A.2 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, è necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante "WPS e Wireless ON/OFF" presenti nel pannello anteriore del prodotto per 5 (o più) secondi, il router riporterà tutte le impostazioni ai valori iniziali (il led Status si spegnerà ed il dispositivo effettuerà il reboot).
2	I parametri di default per l'accesso alla configurazione del Router ADSL sono: Indirizzo IP:192.168.1.254 Username: admin, Password: atlantis Wireless con SSID:A02-RAU242-WN Wireless (WPA2-PSK in AES) con password: WebShare242WN
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.3 Interfaccia LAN

Le schermate di configurazione Web non vengono visualizzate correttamente.

Steps	Azione correttiva
1	Accertarsi di utilizzare Internet Explorer 5 o una versione successiva.
2	Eliminare i files temporanei di Internet ed eseguire un nuovo login.

Non è possible accedere al WebShare Wireless N ADSL2+ Router dalla LAN e nemmeno eseguire un ping dal router verso i PC della rete.

Steps	Azione correttiva
1	Verificare che i LEDs relativi alle porte LAN posti sul pannello frontale del WebShare Router siano accesi in corrispondenza dei cavi di rete collegati. Se entrambi i LEDs sono spenti fare riferimento alla sezione A.1.2.
2	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del WebShare Router .
3	Se è stato modificato l'indirizzo IP lato LAN del Router è necessario modificare L'URL di accesso al prodotto.

4	Se i problemi persistono effettuare un reset dell'apparato.

A.4 Interfaccia WAN(accesso ad Internet)

L'inizializzazione della connessione ADSL fallisce.

Steps	Azione correttiva
1	Verificare che il cavo telefonico e la presa a muro funzionino correttamente. Il LED ADSL dovrebbe essere acceso.
2	Verificare che i valori di VPI e VCI siano corretti, nel dubbio verificare tali parametri con il proprio Provider.
3	Riavviare il Router ADSL. Se il problema persiste contattare l'assistenza tecnica Atlantis.

Non è possibile ottenere un indirizzo IP pubblico dall' ISP.

Steps	Azione correttiva
1	L' indirizzo IP pubblico viene fornito dal Provider dopo l'autenticazione di username e password.
2	Questo tipo di autenticazione si verifica solo con i protocolli PPPoE e PPPoA, verificare quindi che i parametri inseriti siano corretti.

Non è possibile accedere ad Internet.

Steps	Azione correttiva
1	Accertarsi che il Router ADSL sia stato impostato correttamente per la connessione ad Internet.
2	Se il LED WAN è spento fare riferimento alla sezione A.1.3.

La connessione ad Internet si disconnette.

Steps	Azione correttiva
1	Verificare le impostazioni di scheduling della connessione.
2	Se si utilizzano i protocolli PPPoA e PPPoE per la connessione verificare le impostazioni di IDLE-TIMEOUT.
3	Verificare che il valore di SNR (Status-Downstream) sia almeno 12dB nel caso di ADSL.
4	Contattare l'ISP.

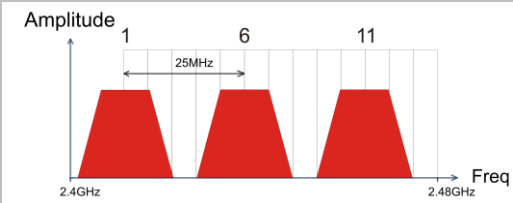
A.5 Interfaccia WLAN

Il client wireless, configurato in DHCP, non riceve l'indirizzo IP dal router.

Steps	Azione correttiva
1	Accertata l'avvenuta connessione con la WLAN del router, provare ad aggiornare i driver del client wireless.
2	Se il problema persistesse, procedere come da punto 3. Talune volte infatti il pacchetto DHCP non riesce a passare a cause di settaggi **RTS/CTS** e **Fragmentation Threshold(bytes).** Tale parametro andrebbe impostato sui driver del client wireless. Riprovare verificando se l'attriobuzione dell'indirizzo IP avviene correttamente. Alternativamente
3	Assegnare al client Wireless un indirizzo IP statico (del tipo 192.168.1.1, subnet=255.255.255.0, DG=192.168.1.254) e provare ad effettuare un ping verso l'indirizzo IP del router.

A.5 Interfaccia WLAN

Steps	Risposta
Posso giocare in rete con gli altri computer presenti sulla WLAN?	Si, se il gioco è dotato di funzionalità multiplayer in rete.

Steps	Risposta
Cos'è lo Spread Spectrum?	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.

Steps	Risposta
Cosa sono DSSS e FHHS?	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHHS (Frequency Hopping Spread Spectrum): è una tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.

Steps	Risposta
Cos'è un decibel?	Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare. L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.
dBm	Definiamo il dBm=10 log 10 (P 2 / P 1), dove P1 =1 milliWatt (mW). E' possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm. Nella tabella seguente è riportata l'equivalenza per i valori più comuni (utilizzare la formula di sopra per valori non in tabella):

dBm	Watt	note
0	1 mW	
3	2 mW	
6	4 mW	
9	8 mW	
10	10 mW	
12	15,8 mW	
13	20 mW	
14	25 mW	

15	32 mW	
16	40 mW	
17	50 mW	
18	63 mW	
19	79 mW	
20	100 mW	Massima Potenza utilizzabile per WLAN a 2.4Ghz
23	200 mW	
26	400 mW	
29	800 mW	

dBi	Il guadagno di un'antenna è definito come il rapporto fra la densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P 2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza. Definiamo il dBi=10 log 10 (P 2 / P isotropica), dBm=10 log 10 (Potenza/ 1mW)
Antenna Isotropica	Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare. L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.
Antenna Direttiva	Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza.

Interferenze sulla WLAN?

Domanda	**Risposta**
Banda ISM	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and

	Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.
Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?	Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze. Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi. In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.
Canali	Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili. E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6). L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**". Il disegno seguente illustra meglio quanto detto: Sino a 3 AP possono coesistere senza overlapping. E' opportuno prestare attenzione all'assegnazione dei canali. Nel caso di 802.11g i canalo sono solo (alto e basso).

Domande Varie ?

Steps	Risposta
WDS	Il WDS (Wireless Distribution System) è la tecnologia che permette ad un Access Point di svolgere contemporaneamente la funzionalità di AP e di Repeater del segnale. Risulta essere

	la soluzione ottimale per estendere la copertura di una wireless LAN in ambienti dove non è assolutamente possibile stendere cavi. Può essere utile per raggiunge relocazioni remote. Va osservato che l'uso di un repeater ha un forte impatto sulle prestazioni dei client wireless ad esso collegati.
IEEE802.11g	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.
Infrastructure	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point.
Sicurezza	L'Access Point offre funzionalità di crittografia WEP fino a 128 bit, ciò provvede a rendere sicure le trasmissioni dati wireless. L'utilizzo del WPA e/o WPA2 rende ancora più sicura la trasmissione wireless. Tali tecnologie devono essere supportate anche dai vari client utilizzati.

A.6 NAS

Protocollo	Come accedere	Home Directory	Struttura directory	
FTP	ftp://IP	C	Download	BT
			Public	
Samba	//IP/Storage		Folder X	
			Folder Y	
			Folder Z	

A.7 Varie

La navigazione avviene senza problemi ma l'invio di allegati nelle mail crea problemi.

Steps	Azione correttiva
1	Accedere via WEB al Router, cliccare su **Basic->Networking->Internet Setup** e cambiare la voce MTU Option in 1450 (anziché il valore 0 di default).
2	Contattare il proprio Internet Service Provider e verificare che non siano presenti problematiche sulle infrastrutture di rete.
3	Riavviare il Router ADSL. Se il problema persiste contattare l'assistenza tecnica Atlantis.

La navigazione avviene senza problemi ma le prestazioni di Emule (programmi di p2p) non sono soddisfacenti.

Steps	Azione correttiva
1	Accedere via WEB al Router, cliccare su **Advanced ->Forwarding Rules->Virtual Server** e creare 2 regole che ruotino le porte usate da Emule sull'IP del PC (deve essere statico) su cui Emule sta funzionando.
2	Verificare che Emule (la procedura va bene per qualsiasi altro software) usi effettivamente le porte di sopra. Atlantis non potrà fornire supporto (sulle porte utilizzate) che andrà richiesto al produttore del software in questione.
3	E' opportuno considerare che programmi del genere creando un numero di connessioni simultanee molto alto possono rallentare enormemente la navigazione e portare il router in uno stato di blocco. In qusto caso limitare l'uso di tali programmi e/o configurarli limitando le connessioni simultanee.
4	Contattare il proprio Internet Service Provider e verificare che non siano presenti blocchi particolari per i programmi di p2p.

La navigazione avviene senza problemi ma l'invio di allegati nelle mail crea problemi.

Steps	Azione correttiva
1	Accedere via WEB al Router, cliccare su **Basic->Primary Setup** e cambiare la voce MTU Option in 1450 (anziché il valore 1492 di default).
2	Contattare il proprio Internet Service Provider e verificare che non siano presenti problematiche sulle infrastrutture di rete.
3	Riavviare il Router ADSL. Se il problema persiste contattare l'assistenza tecnica Atlantis.

La navigazione avviene senza problemi ma le prestazioni di Emule (programmi di p2p) non sono soddisfacenti.

Steps	Azione correttiva
1	Accedere via WEB al Router, cliccare su Advanced Settings->Forwarding Rules->Virtual Server e creare 2 regole che ruotino le porte usate da Emule sull'IP del PC (deve essere statico) su cui Emule sta funzionando.
2	Verificare che Emule (la procedura va bene per qualsiasi altro software) usi effettivamente le porte di sopra. Atlantis non potrà fornire supporto (sulle porte utilizzate) che andrà richiesto al produttore del software in questione.
3	E' opportuno considerare che programmi del genere creando un numero di connessioni simultanee molto alto possono rallentare enormemente la navigazione e portare il router in uno stato di blocco. In qusto caso limitare l'uso di tali programmi e/o configurarli limitando le connessioni simultanee.
4	Contattare il proprio Internet Service Provider e verificare che non siano presenti blocchi particolari per i programmi di p2p.

Domanda	Risposta
Cos'è il Wake on Lan?	Tale funzionalità consente il risveglio del PC tramite opportuni pacchetti provenienti dalla LAN locale. Le condizioni da rispettare per poter utilizzare pienamente questa funzionalità sono: • Scheda di rete con funzionalità WoL • Piastra madre che supporti tale funzionalità e che sia abilitata (accedendo al Bios in genere è sufficiente abilitare la voce Wake on Lan) • Alimentatore che sia in grado di fornire una corrente di standby di almeno 600/700 mA ATX • Desktop management software che invia I pacchetti "wake-up" ai PC Un PC che supporta, tramite i componenti di sopra, la funzionalità Wake-On-LAN non è mai completamente "spento" dato che deve comunque mantenere attivi alcuni componenti. Se pertanto il PC venisse spento staccando il cavo di alimentazione dalla rete elettrica e poi ricollegato, la funzionalità WoL non funzionerebbe perché lo stato del PC sarebbe differente rispetto ad uno spegnimento non forzato. Benché il PC sia spento la scheda di rete deve comunque sempre monitorare la LAN in attesa di un eventuale pacchetto di wake-up. Ricevuto il pacchetto la scheda segnala alla piastra madre di effettuare la riaccensione del PC. Non è necessario conoscere l'indirizzo IP della scheda. Tutti i software sono liberamente scaricabili all'indirizzo

	www.depicus.com, cliccare su Wake on Lan e scaricare il software appropriato.

Domanda	**Risposta**
Cos'è il Remote Wake on Lan?	Utilizzando Magic Pocket è possibile "risvegliare" PC della LAN dietro al Router ADSL da un qualsiasi PC con una connessione internet. Per ulteriori dettagli scaricare la guida apposita nella sezione Approfindimenti del prodotto.

Domanda	Risposta
Non funziona il Server settato su un PC della LAN privata.	Il Router ADSL applica, ad ogni pacchetto, nell'ordine: • Firewall • Virtual Server • DMZ Affichè il Server funzioni bisogna accertarsi che nessun blocco antecedente al VS (Firewall) o DMZ (Firewall e VS) operi in non conformità. Settare il PC che funge da Server con un indirizzo IP privato fisso (o usare la modalità Fixed Host nel DHCP)..

Domanda	Risposta
Posso giocare in rete con gli altri computer presenti sulla WLAN?	Si, se il gioco è dotato di funzionalità multiplayer in rete.

Domanda	Risposta
Cosa fa esattamente il NAT?	Nat significa Network Addsress Traslation (traslazione degli indirizzi di rete locale). E' stato proposto e descritto nell'RFC-1631 ed aveva, almeno originariamente, il compito di permettere uno sfruttamento intensivo degli indirizzi IP. Ogni strumento che realizzi il NAT è composto da una tabella costruita da coppie di indirizzi IP, uno della rete privata ed uno pubblico. Dunque c'è una traslazione dagli IP della rete privata a quelli pubblici ed il contrario. L' Adsl2+ VPN Router supporta il NAT, pertanto con un'opportuna configurazione più utenti possono accedere ad Internet usando un singolo account (e un singolo IP pubblico). Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Il Nat inoltre è una sorta di primo firewall che migliora la sicurezza della Lan locale. Andrebbe usata quando il traffico indirizzato verso Internet è una parte di quello che circola nella Lan locale, altrimenti tale funzionalità potrebbe degradare leggermente le prestazioni della connessione ad Internet. Tale funzionalità coesiste con la funzionalità Virtual Server, DMZ e DHCP. Il Nat manipola i pacchetti IP uscenti e ne cambia il campo **IP provenienza**

	sostituendo il mittente del pacchetto (in questo caso l'indirizzo IP il PC della Lan, che è un IP privato non valido in Internet) con l'IP pubblico dell' Adsl2+ VPN Router. In questo modo tutti i pacchetti uscenti dal Router avranno nel campo mittente l'indirizzo IP pubblico del Router. Quando poi i pacchetti torneranno al Router questo in base a tabelle memorizzate provvederà al processo contrario e li spedirà al PC interessato nella Lan.

Domanda	Risposta
Alcune applicazioni, quando il Router fa NAT oppure è attivo il firewall, potrebbero non funzionare propriamente.	Il Router, tramite il NAT e/o il firewall, protegge la LAN isolandola dall'esterno e rifiutando tutti i tentativi di connessione generati dall'esterno. In Internet ogni servizio è associato ad una porta. Queste porte potrebbero essere chiuse per evitare che malintenzionati possano accedere alla LAN. Tuttavia può essere necessario, per il funzionamento di determinate applicazioni (ad esempio NetMeeting), che i tentativi di connessione generati dall'esterno su determinate porte siano rigirati ad un PC della LAN su cui il programma in questione sia in "ascolto". Consultare la sezione Virtual Server per avere maggiori dettagli. Le applicazioni che tipicamente dovranno essere configurate sono: • Alcuni Programmi di Email • Alcuni Giochi Multi-Players • Alcune Applicazioni Phone/Video Conferenza Per trovare le porte da aprire per il corretto funzionamento dell'applicazione solitamente la strada più breve è quella di consultare il sito web del produttore dell'applicazione stessa. Resta inteso che in questo modo un solo PC della LAN (quello su cui saranno girate le opportune porte) potrà usare l'applicazione in questione.

Domanda	Risposta
Per effettuando la rotazione delle porte col VS l'applicazione non funziona correttamente, cosa posso fare?	Potrebbe rendersi necessario effettuare una DMZ verso il PC su cui si vuole far girare una particolare applicazione.

Pur utilizzando la DMZ l'applicazione non funziona ancora, che soluzioni adottare?	Nonostante le caratteristiche del Router alcune applicazioni potrebbero non funzionare perché non trasparenti al NAT (nemmeno effettuando una DMZ). In questo caso è possibile utilizzare il Router in modalità Bridge. Così facendo l'indirizzo IP pubblico del Router viene "dato" al PC che dunque potrà far funzionare tutte le applicazioni (come se il Router fosse un modem ADSL).

Domanda	Risposta
Le performance in download o in upload non sono allineate col tipo di contratto offerto dall'ISP.	Assicurarsi che il cavo ADSL sia (in ogni suo punto) ad almeno 30cm da qualsiasi alimentatore. Allontanare il Router da qualsiasi apparecchio che possa generare campi elettromagnetici (Computer con lo chassis aperto, monitor CRT, cellulari) ed interferire. Qualora non si ottenesse il risultato sperato controllare il proprio contratto (**vedere la banda minima garantita**) ed eventualmente contattare l'ISP. Se i problemi continuassero, contattare l'assistenza tecnica di Atlantis spa.

Domanda	Risposta
Perché il Router si connette automaticamente all'ISP?	Il Router ADSL genera una connessione quando un PC della Lan invia un pacchetto (funzione di Dial on Demand) indirizzato ad un indirizzo IP differente da quello della sua classe di appartenenza. Questo fenomeno deve essere controllato in caso di abbonamento non Flat.

Domanda	Risposta
A cosa serve il DDNS?	Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnetterà, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile (ad esempio) ospitare un sito WEB sul proprio PC, effettuare configurazioni da remoto e utilizzare il Router come server VPN. I passaggi da seguire sono i seguenti: • Registrare il proprio dominio (ad esempio) gratuitamente www.dyndns.org. L'operazione richiederà qualche

	minuto. • Configurare il client sul Router inserendo i campi appropriati (Domain Name, Username e Password). Attenzione alla configurazione del campo Period (il Router aggiorna il server DDNS usando come parametro il campo Period, oltre che ogni volta che riceve dalla sfida PPPoA/PPPoE un nuovo indirizzo IP) nel rispetto delle policy del gestore DDNS. • Configurare il Virtual Server affinché rigiri sull'indirizzo IP del PC (di sopra) predisposto le connessioni provenienti dall'esterno In questo modo ogni utente che voglia connettersi all'indirizzo registrato interrogherà il server DDNS che gli restituirà di volta in volta l'indirizzo IP datogli dal Router cui lo ha assegnato l'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente. In questo modo se il PC resta sempre acceso il server WEB è di fatto sempre raggiungibile (se si escludono problemi diversi).

Domanda	**Risposta**
Pur avendo bloccato alcuni siti con la funzione URL blocking, è comunque possibile accedervici. Come mai?	Attenzione al fenomeno del reindirizzamento dei siti che può permettere il non corretto funzionamento del servizio. Es: il sito www.libero.it è reindirizzato verso www.iol.it, quindi bloccando libero.it, la servizio sarà efficace solo bloccando anche www.iol.it, altrimenti essendo quest'ultimo tra i consentiti, ne permetterà la navigazione e quindi annullerà il blocco su libero.it.

Domanda	**Risposta**
Voglio accrescere la sicurezza dle Router abilitando la funzionalità SPI?	Tale funzionalità consente, utilizzando l'hardware del Router, di impedire ogni tipo di accesso indesiderato. Per abilitarla è sufficiente entrare nel router e configurare la sezione Intrusion Detection del Firewall. Con questa funzionalità attiva l'intera Lan sarà ulteriormente protetta poiché ogni pacchetto in transito viene esaminato a fondo e tutti i pacchetti di risposta vengono confrontati ed esaminati prima di essere inoltrati (di ogni pacchetto viene fatto una sorta di hash particolare che ne certifica l'autenticità).

	Nota Bene: Alcune applicazioni internet potrebbero non funzionare correttamente con tale funzionalità attivata.

Domanda	**Risposta**
Che caratteristiche ha un attacco Denial of Service?	Lo scopo di attacchi di questo tipo non è quello di cogliere informazioni particolari dalla vostra rete quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Più precisamente esistono 4 specifici tipologie di attacchi DoS. • Attacchi che mirano all'esaurimento della banda, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente può usare altri host che di fatto amplificano l'attacco. • Attacchi che mirano all'esaurimento delle risorse. • Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware. • Attacchi DoS generici. Il Router può automaticamente rilevare e bloccare un attacco di tipo DoS (Denial of Service) se questa funzione è attiva.

Domanda	**Risposta**
Quali porte è opportuno aprire nel Firewall per il corretto funzionamento del servizio DDNS?	Generare una regola che consenta in uscita la porta 8245 in TCP (oltre alla canonica 80 in TCP).

Domanda	**Risposta**
Quali porte è opportuno aprire nel Firewall per il corretto funzionamento del servizio SNMP?	Generare una regola che consenta in uscita la porta 161 UDP.

Domanda	Risposta
Come posso rendere il Router permanentemente configurabile da remoto?	La funzionalità Remote Access permette l'accesso per un tempo limitato. Impostando il valore a "0" l'accesso è sempre consentito, ma al primo riavvio del dispositivo, per ragioni di sicurezza, tale settaggio viene cancellato. E' però possibile creare delle regole nel Virtual Server che ruotino la porta sull'IP del Router ADSL. Ad esempio ruotando la porta 80/TCP si abilita permanentemente la configurazione remota via WEB. Nel caso la porta 80 venisse utilizzata per un server WEB è sufficiente cambiare la porta di configurazione del Router e ruotarla nel Virtual Server.

Domanda	Risposta
Cos'è l'UPnP?	Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di configurarsi automaticamente senza l'intervento dell'utente. Chiunque dunque sarà in grado, senza conoscere complicati concetti, di godere pienamente dei vantaggi del NAT e contemporaneamente utilizzare le più comuni applicazioni Internet senza il minimo problema.

6. SUPPORTO OFFERTO

Per qualunque altro problema o dubbio sul funzionamento del prodotto, è possibile contattare il servizio di assistenza tecnica Atlantis tramite l'apertura di un ticket on-line sul portale http://www.atlantis-land.com/ita/supporto.php.

Nel caso non fosse possibile l'accesso al portale di supporto, è altresì possibile richiedere assistenza telefonica al numero 02/ 78.62.64.37 (consultare il sito per verificare gli orari in cui il servizio viene erogato).

Per esporre eventuali richieste di supporto prevendita o richieste di contatto , si invita ad utilizzare gli indirizzi mail info@atlantis-land.com oppure prevendite@atlantis-land.com.

Atlantis SpA
Via S. Antonio, 8/10
20020 Lainate (MI)
Fax: +39.02.78.62.64.39
Website: http://www.atlantis-land.com
Email: info@atlantis-land.com

APPENDICE A: Connessione usando il Client di Windows

In Windows XP/Vista e 7 è incluso un client che permette la gestione di un adattatore wireless al pari delle Utility.

Windows 7

- Cliccare sull'icona di rete posizionata sulla System Tray (vedi immagine) e selezionare l'opzione **Centro connessioni di rete e condivisione** oppure cliccare su **Start -> Pannello di Controllo -> Centro connessioni di rete e condivisione**.

- Selezionare l'opzione **Connessione a una rete** dal menu di sinistra per visualizzare la lista di reti wireless disponibili.
- Selezionare l'SSID della rete **A02-RAU242-WN** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPA2-PSK,** Encrypton: **AES**, Encryption Key: **WebShare242WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB all'AP.

	Nel caso in cui non sia possibile visualizzare la lista di reti senza fili disponibili, si prega di verificare la corretta installazione dei driver del client USB.

Windows VISTA

- Cliccare sull'icona di rete posizionata sulla System Tray (vedi immagine) e selezionare l'opzione **Centro connessioni di rete e condivisione** oppure cliccare su **Start -> Pannello di Controllo -> Centro connessioni di rete e condivisione**.

- Selezionare l'opzione **Connessione a una rete** dal menu di sinistra per visualizzare la lista di reti wireless disponibili.
- Selezionare l'SSID della rete **A02-RAU242-WN** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPA2-PSK,** Encrypton: **AES**, Encryption Key: **WebShare242WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB all'AP.

	Nel caso in cui non sia possibile visualizzare la lista di reti senza fili disponibili, si prega di verificare la corretta installazione dei driver del client USB.

Windows XP

- Fare doppio click sull'icona di rete posizionata sulla System Tray (vedi immagine).

- Selezionare l'SSID della rete **A02-RAU242-WN** (utilizzare le seguenti impostazioni per la sicurezza: Authentication: **WPA2-PSK,** Encrypton: **AES**, Encryption Key: **WebShare242WN**) e premere sul pulsante **Connetti** per avviare la procedura di connessione.

Al termine della procedura di connessione, un messaggio confermerà l'avvenuta connessione del client USB all'AP.

Di seguito è indicato come disabilitare il servizio Zero Configuration di Windows XP, al fine di poter controllare il dispositivo tramite l'utility fornita a corredo:

- Cliccare su **Start** e poi su **Pannello di Controllo**
- Selezionare dal menu di sinistra la voce **Visualizzazione classica**
- Cliccare su **Strumenti di amministrazione**
- Cliccare su **Servizi**
- Selezionare il servizio **Zero Configuration** e cliccare su **Proprietà**
- Cliccare sul pulsante **Arresta** per terminare temporaneamente il servizio

Impostare il campo **Tipo di Avvio** su **Disabilitato** come da figura

APPENDICE B: Dynamic DNS (DynDNS)

Grazie all'adozione di questa features è possibile registrare un dominio pur se associato ad un IP dinamico. Ci sono una moltitudine di server DDNS che offrono gratuitamente questo tipo di servizio. E' sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che consentirà di raggiungere (da remoto) sempre il WebShare Wireless ADSL2+ Router . E' possibile in questo modo effettuare facilmente configurazioni da remoto, ospitare un sito WEB o FTP.
Ogni qual volta il WebShare Wireless ADSL2+ Router si riconnetterà, tramite il client incorporato, comunicherà al server DDNS il nuovo indirizzo IP. In questo modo chiunque dall'esterno conoscendo l'URL conoscerà anche l'indirizzo IP che in quel momento è stato assegnato al WebShare Wireless ADSL2+ Router .
Vediamo, nel dettaglio come effettuare una registrazione con il gestore DDNS forse più famoso.
Andare nel sito:www.dyndns.org, cliccare su **Account.**

Effettuare la registrazione (cliccando su **Create Account**) inserendo: **Username, Indirizzo Mail e Password.**
Una mail di verifica registrazione sarà inviata all'indirizzo inserito. In questa mail sono contenute le istruzioni per proseguire la registrazione (è necessario confermare

così il tutto entro 48 ore). Seguire le istruzioni contenute e compilare il form per terminare la fase di registrazione.
A questo punto tornare nel sito, andare su **Services**, evidenziare (nella parte sinistra) il menù **Dynamic DNS** e poi cliccare su **Add Host**.
Non resta che introdurre il **Nome dell'host** (evidenziare Enable WildCard) e scegliere il suffisso preferito e premere poi sul bottone **Add Host** per terminare.
Passiamo adesso alla configurazione del client nel WebShare 142WN.

Andando sul sito www.dyndns.org, (effettuare il LogIn ed andare nella sezione Account poi sotto Dynamic DNS all'URL) è possibile controllare che l'IP sia stato aggiornato (alternativamente è possibile effettuare un ping verso l'URL registrato).

APPENDICE C: Packet Filter

Il WebShare 142W dispone di un sofisticato Packet Filter col quale riesce ad esaminare tutto il traffico che lo attraversa. In questo modo è possibile, conoscendo le caratteristiche dei pacchetti IP associati ai più comuni servizi, effettuare i filtraggi in maniera corretta. In questa appendice verranno evidenziate le varie modifiche subite da un pacchetto durante il percorso.
Verranno utilizzate le seguenti convenzioni:

- **BLU** per indicare una INVERSIONE
- **ROSSO** per indicare un CAMBIAMENTO

Condizioni di partenza:

- NAT attivo
- PCX della LAN con IP 192.168.1.X
- Router con LAN IP 192.168.1.254

Il caso da esaminare prevede una LAN in cui il PC con IP 192.168.1.X vuole visualizzare un sito WEB.

Vi sono 2 fasi:Risoluzione dell'URL (tale valore potrebbe essere recuperato in qualche cache o fornito da appositi programmi, ma per completezza verrà affrontato il caso più comune) e costruzione della connessione TCP col sito WEB.

Il primo pacchetto è inviato dal PC (con IP 192.168.1.X) verso il server DNS per chiedere la risoluzione dell'URL cercato.

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Questo pacchetto uscente arriva al WebShare 142W che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendo il suo IP Pubblico e lo inoltra al server DNS.

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	C	
	Porta Destinazione	53	

Arrivato al server DNS il pacchetto torna indietro, reindirizzato al WebShare 142W (che ne aveva cambiato prima l'IP di provenienza). Sono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello UDP.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	**IP del Server DNS**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	**53**	
	Porta Destinazione	**C**	

Arrivato al WebShare 142W, il pacchetto viene riprocessato ed inviato al PC di provenienza.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	IP del Server DNS	
	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo UDP	UDP
	Porta Provenienza	53	

	Porta Destinazione	C	

A questo punto, dal pacchetto UDP arrivato, il PC (con IP 192.168.1.X) ha risolto l'URL e conosce l'indirizzo IP associato. Inizia dunque la fase della costruzione della connessione TCP (il protocollo TCP infatti richiede la costruzione della connessione, al contrario di quello UDP).

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Questo pacchetto uscente arriva al Router che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendovi il suo Pubblico e lo inoltra al server WEB.

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	**IP lato WAN del Router**	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	K	
	Porta Destinazione	80	

Arrivato al server WEB il pacchetto torna indietro, reindirizzato all' WebShare ADSL2+ Router (che ne aveva cambiato prima l'IP di provenienza). Vengono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello TCP.

	Direzione Pacchetto	Internet- Router [Entrante]	
IP	IP Provenienza	**IP URL**	
	IP Destinazione	**IP lato WAN del Router**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	**80**	
	Porta Destinazione	**K**	

Arrivato all’ WebShare ADSL2+ Router il pacchetto viene riprocessato ed inviato all’IP di provenienza.

	Direzione Pacchetto	Router-PC[Entrante]	
IP	IP Provenienza	IP URL	
	IP Destinazione	**192.168.1.X**	
	Pacchetto contenuto	Tipo TCP	TCP
	Porta Provenienza	80	
	Porta Destinazione	K	

E’ stato evidenziato tanto il percorso dei pacchetti che le trasformazioni che questi subiscono. Nell’esempio di sopra si sono utilizzati dei parametri C e K. Sono dei numeri interi >1024. Nei protocolli per porta quali TCP/UDP infatti il mittente parla ad una porta di destinazione (su cui è in ascolto il server) ed indica una porta (la porta di provenienza appunto) dove aspetta la risposta. Il pacchetto una volta ricevuto dal server viene reinviato al mittente sulla porta su cui questo aspetta la risposta (viene effettuata un’inversione a livello di porte).

APPENDICE D: Classe Pubblica

Grazie a questa funzionalità è possibile gestire più interfacce LAN. Solitamente la tipologia di contratti offerti dall'ISP ricade entro una delle seguenti tipologie:

- A=1 Indirizzo IP Dinamico, in genere offerto con PPPoA/PPPoE
- B=1 Indirizzo IP statico, in genere offerto con RFC1483 Routed
- C=N Indirizzi IP statico, in genere offerto con RFC1483 Routed

Solitamente la punto-punto è routata e pubblica. N è un multiplo di 8.

In figura sono riportate le possibili configurazioni del Router:

Tipo Abbonamento	WAN	LAN	Virtual Computer
1 Indirizzo IP Dinamico **(Tipo A)**	Va configurata con i dati della punto-punto con NAT attivo.	Va configurata con una classe privata che verrà nattata sull'IP pubblico della WAN.	N/A
1 Indirizzo IP statico **(Tipo B)**	Va configurata con i dati della punto-punto con NAT attivo.	Va configurata con una classe privata che verrà nattata sull'IP pubblico della WAN.	N/A
N indirizzi IP statici **(Tipo C)**	Va configurata con i dati della punto-punto con NAT NON attivo.	Va configurata conil primo degli IP della classe pubblica.	N/A

Segue nel dettaglio la configurazione dell'ultimo caso (TIPO **C**).
Per ipotesi il contratto con l'ISP sia il seguente:

Punto-Punto Routata Pubblica

- IP Lato Router(WAN IP)=80.80.80.214
- Default Gateway=80.80.80.213
- Subnet Mask=255.255.255.252

Classe di 8 IP Pubblici

- 8 IP, il cui primo è 81.38.28.64
- subnet 255.255.255.248

Si ricorda che il primo e l'ultimo IP non vanno utilizzati (nel caso in esame 81.38.28.64 e 81.38.28.71), è pertanto possibile utilizzare dall'IP 81.38.28.65-81.38.28.70.

La configurazione procede nei seguenti passi:

Configurazione della WAN: Scegliere **RFC1483 Routed** impostando l'incapsulazione in **LLC**. Introdurre poi i dati della punto-punto ed infine cliccare su **Save.**

WAN Type	IP over ATM Change...
WAN IP Mode	Static IP Address
WAN IP Address	80.80.80.214
WAN Subnet Mask	255.255.255.252
WAN Gateway	80.80.80.213
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
IGMP	Enable
NAT	Disable
Data Encapsulation	LLC
VPI Number	8 (range: 0~255)
VCI Number	35 (range: 1~65535)
Schedule type	UBR
Save Undo Virtual Computers...	

Attenzione il NAT deve essere spuntato.

Configurazione della LAN:

Tipo Abbonamento	IP	Default Gateway	DNS
Router*	81.38.28.65/ 255.255.255.248	N/A	Inseriti
PC 1	81.38.28.66/ 255.255.255.248	81.38.28.65	Inseriti
PC 2	81.38.28.67/ 255.255.255.248	81.38.28.65	Inseriti
PC 3	81.38.28.68/ 255.255.255.248	81.38.28.65	Inseriti
PC 4	81.38.28.69/ 255.255.255.248	81.38.28.65	Inseriti
PC 5	81.38.28.70/ 255.255.255.248	81.38.28.65	Inseriti

*Questo è l'IP Lato LAN del Router configurabile in **Advanced->Basic Settings->Network Setup->Lan IP Address**

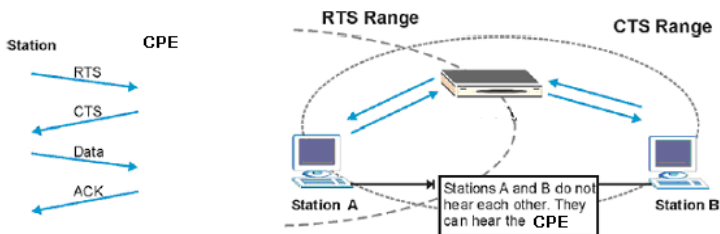
APPENDICE E: Rete Wireless

Introduzione alla rete Wireless
Questa sezione presenta la Wireless Lan e alcune configurazioni di base. Una Wireless Lan può essere creata semplicemente con due computer dotati di schede di rete Wireless che comunicano in una rete di peer-to-peer oppure in maniera più complessa utilizzando più computers con schede di rete senza fili che comunicano attraverso punti di accesso che fanno da ponte tra la rete Wireless e la rete cablata.

Canali
Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).

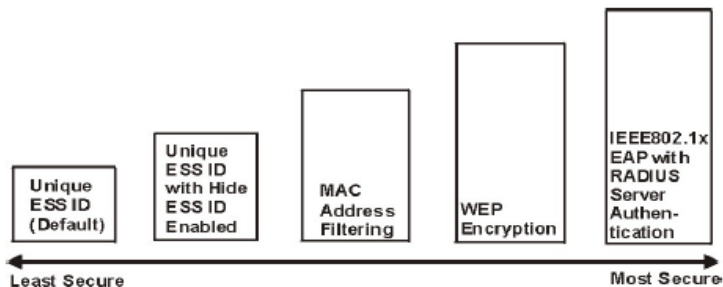
- Quando si utilizza lo standard B/G i canali senza Overlap in frequenza sono 3 (i canali 1,6,11 possono coesistere senza problemi contemporaneamente ed in sovrapposizione spaziale)
- Quando si utilizza lo standard N i canali senza Overlap in frequenza sono solo 2 (i canali alto/basso possono coesistere senza problemi contemporaneamente ed in sovrapposizione spaziale)

ESS ID
L' Extended Service Set (ESS) consiste in un gruppo di Access Point o Gateway Wireless connessi ad un LAN cablata sulla stessa subnet. Un ESS ID identifica univocamente ogni gruppo. Ciascun Access Point o Gateway Wireless e le stazioni Wireless a loro associate devono avere lo stesso ESSID.

RTS/CTS
Quando due stazioni Wireless sono all'interno del range dello stesso Access Point ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.

La stazione A invia dei dati al Router ADSL ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono all'Access Point.
Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS all' Access Point per ottenere il permesso ad iniziare. L'Access Point invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.

Fragmentation Threshold (Soglia di frammentazione)
Il Fragmentation Threshold è la dimensione massima di frammentazione dei dati (tra 256 e 2432 bytes) che può essere trasmessa in una rete Wireless prima che il Router ADSL effettui un ulteriore divisione in frames più piccoli.
Un alto valore di Fragmentation Threshold è indicato per reti esenti da interferenze, mentre per reti soggette ad interferenze e con un traffico molto elevato è preferibile optare per un valore più basso.
Se viene impostato un valore più basso dell'RTS/CTS i dati verranno frammentati prima della fase di handshake la quale non verrà effettuata.

Livello di Sicurezza
Le funzionalità di Wireless Security sono necessarie per proteggere le comunicazione tra stazioni Wireless , Access Point e la rete cablata.

La figura sotto indica i possibili livelli di sicurezza Wireless firniti dal Router ADSL. Il livello di sicurezza più alto conta sul protocollo EAP (Extensible Authentication Protocol) per l'autenticazione ed utilizza WEP con scambio di chiavi dinamico. Questo sistema richiede l'interazione con un server RADIUS (Remote Authentication Dial-In User Service) che offre servizi di autenticazione per stazioni Wireless.

Se none viene utilizzato alcuna funzionalità di Wireless Security il Router ADSL sara accessibile da qualsiasi stazione Wireless presente nel suo campo di azione. E' possibile configurare questo servizio tramite l'interfaccia di configurazione Web del prodotto.

Cifratura dati con WEP/WPA

La cifratura WEP provvede al crittaggio dei dati trasmessi sulla rete in modo da ottenere una comunicazione privata. Il crittaggio viene effettuato sia su comunicazioni unicast che multicast.

Tutte le stazioni Wireless che utilizzano questa cifratura devono utilizzare la stessa chiave per la cifratura e la decodifica dei dati. Il Wireless Router è in grado di utilizzare chiavi di criptaggio da 64 e 128 bit.

Con lo standard G è stato introdotta la cifratura WPA (TKIP) e WPA2 (AES) ritenuta decisamente più sicura che non la cifratura WEP.

APPENDICE F: Copertura

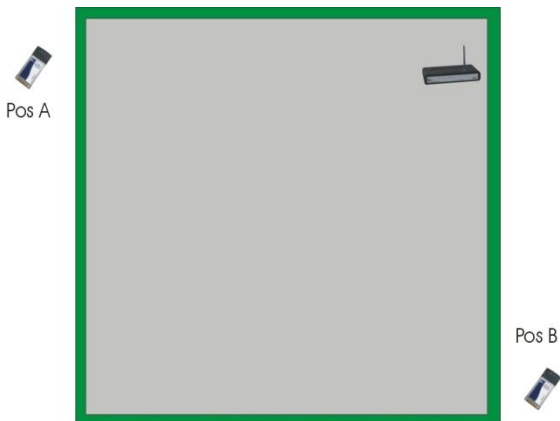
Considerazioni Generali

In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire diverse decine di metri. E’ però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell’interferenza con altri apparati operanti sulle frequenze vicine.
Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

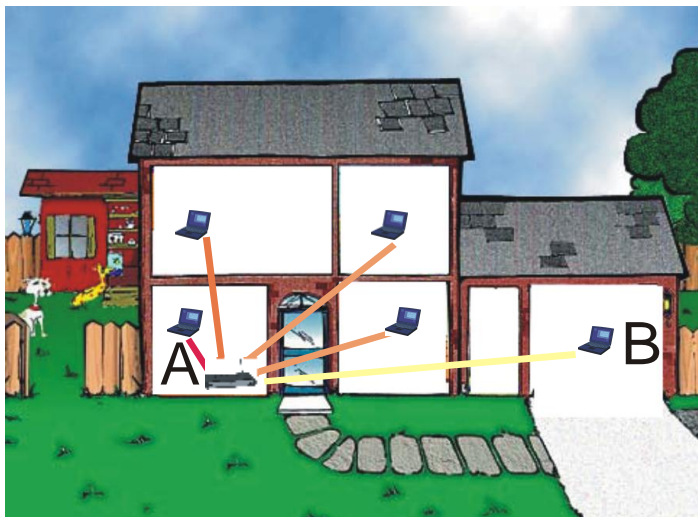
- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.

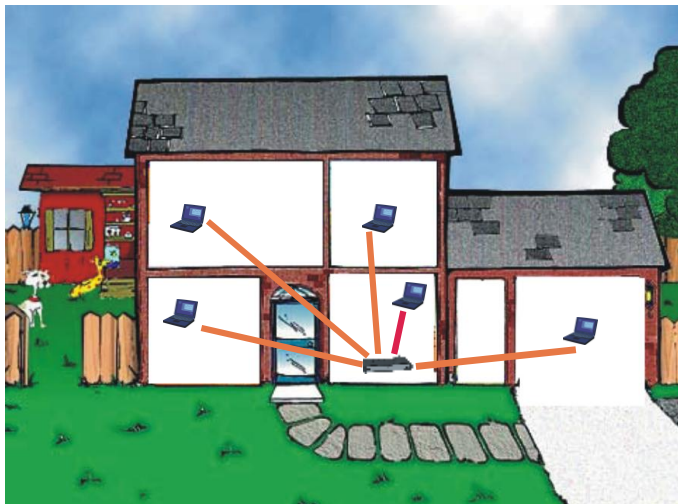
- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E’ bene prendere in considerazione questo fatto.

- Allontanare l’AP Wireless da ogni altro dispositivo che produca emissioni RF.

- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless AP col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un’attenuazione importante). Si veda la figura sottostante:

Il Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A, benché la distanza effettiva dall'AP sia quasi identica nei 2 casi. E' sufficiente collocare il Wireless AP al centro del locale per migliorare decisamente le prestazione del client B.

Dove installare un AP

Immaginiamo di avere un'installazione come quella in figura.

Sicuramente Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A.

E’ sufficiente collocare il Wireless Router/AP al centro della rete per migliorare decisamente le prestazione di entrambi i client B.

Si è operato sulla diminuzione 2 fattori:

- Distanza media
- Sezioni di muro attraversate

E' decisamente meglio avere una rete i cui client abbiano un link mediamente buono che non una rete con taluni client con link eccellente ed altri con link molto scarso.

La stazione lontana, che generalmente trasmette con un data rate più basso, tende a consumare un «airtime» elevato.

L'AP ha meno tempo da dedicare a client più vicini e più veloci.

Prestazioni complessivi peggiori.

APPENDICE G: WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) è un insieme di specifiche mirate a facilitare notevolmente le operazioni di aggiunta di dispositivi alla propria rete wireless e la messa in sicurezza della stessa con la sola pressione di un pulsante oppure tramite l'immissione di un codice PIN.
I dispositivi conformi alle specifiche WPS sono quindi in grado, in maniera molto semplice, di rilevare le reti con tale supporto, acquisirne le impostazioni basilari(quali SSID e canale) e negoziare in maniera del tutto automatica un profilo di sicurezza utiizzando i più avanzati algoritmi di crittografia come WPA e WPA2.
Nella configurazione PIN, un codice PIN univoco viene assegnato ad ogni dispositivo che deve far parte della rete; un adesivo o un etichetta posta sulla parte posteriore del client identificheranno tale codice in caso di PIN statico, o in alternativa questo verrà generato in maniera dinamica e visualizzato tramite utility.
Questo codice viene utilizzato per assicurare l'identificazione univoca della periferica e per evitare intrusioni all'interno della rete da parte di periferiche esterne. Gli utenti, per poter aggiungere il dispositivo alla rete, dovranno inserire all'interno del Registar (presente all'interno dell'Access Point), il codice PIN identificativo della periferica da connettere.
Nella configurazione PCB, l'utente sarà in grado di aggiungere periferiche e mettere in sicurezza la propria rete tramite la semplice pressione di un pulsante (fisico sugli Access Point e virtuale sui dispositivi client).
Di seguito una tabella riassuntiva sui vantaggi del supporto WPS e sulle modalità di configurazione:

Senza WPS	**Con WPS (PIN mode)**	**Con WPS (PCB mode)**
Accensione dell'Acces Point	Accensione dell'Acces Point	Accensione dell'Acces Point
Accesso all'Access Point	Attivazione del client	Attivazione del client
Configurazione dell'SSID	Generazione in maniera automatica dell'SSID e broadcasting della stessa.	Generazione in maniera automatica dell'SSID e broadcasting della stessa.
Attivazione della sicurezza	Accesso al Registar presente sull'Access Point	Pressione del bottone sull'Access Point e sul client
Impostazione della parola di accesso (WPA) o delle chiavi di accesso (WEP)	Insierimento del PIN relativo al client da aggiungere.	
Attivazione del client	Avvio della	

	sincronizzazione tra AP e client	
Selezione della rete a cui connettersi		
Inserimento della chiave di sicurezza per la connessione del client		

APPENDICE H: MAPPATURA DI RETE

Anzitutto è opportuno connettere una periferica di memorizzazione.

- Verificare che sia stata riconosciuta **(Status->Peripheral Status->Ready)**

Peripheral Status

Item	Peripheral Status
USB Device	Ready

- Procedere alla sua formattazione. Il processo può impiegare diverso tempo (il LED Status deve essere fisso).

Disk Distribution

Disk Total Capacity = 7948 MB

Partition	Free(MB)	Used(MB)	Total(MB)
1 [EXT3]	7315	144	7460

*Warning! Formatting will erase all data on this partition.

Format | Check

Creazione della Connessione Remota in Windows XP

In Windows XP è possibile creare la connessione di Rete operando come segue:

- **Start->Pannello di Controllo.**
- Cliccare sul menu **Strumenti** e poi **Connetti unità di Rete.**
- Cliccare su **Sfoglia**, poi selezionare sotto **WorkGroup** il nome precedentemente attribuito all'apparato e poi la cartella **Storage** e cliccare su **OK**.
- Spuntare la voce **Riconnetti all'avvio**.
- Cliccare su **OK.** Non è richiesta alcuna password, salvo che non sia stato impostato il controllo d'accesso **(NAS->Access Control->Authorization Mode).**
- Cliccare poi su **Fine.**

A questo punto è possibile accedere al disco inserito nel WebShare (utilizzando la cartella **Storage**) come fosse un disco del proprio PC.

	In caso di problemi è possibile forzare direttamente l'indirizzo IP dell'apparato per la mappatura di un'unità di rete usando la sintassi **\\192.168.1.254\Storage** nel campo **Cartella.** Cliccare su **OK.** Cliccare poi su **Fine.**

Creazione della Connessione Remota in Windows Vista

In Windows Vista è possibile creare la connessione di Rete operando come segue:

- **Start->Computer**
- Cliccare su **Connetti unità di Rete.**

Connetti unità di rete

Specificare la cartella di rete di cui eseguire il mapping.

Specificare la lettera dell'unità per la connessione e la cartella a cui connettersi:

Unità: Y:

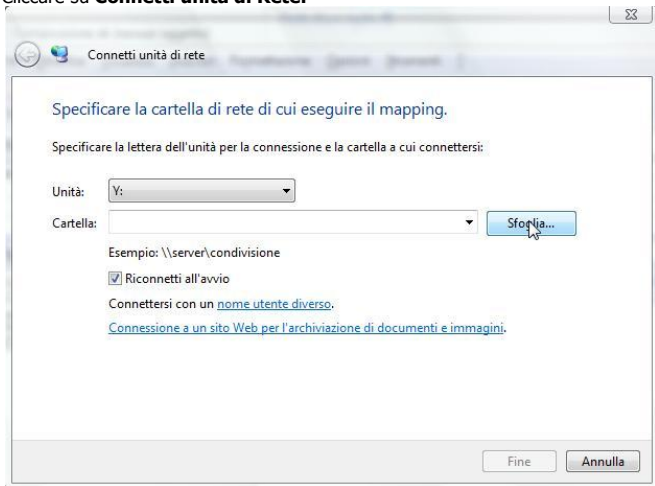
Cartella: Sfoglia...

Esempio: \\server\condivisione

Riconnetti all'avvio

Connettersi con un nome utente diverso.

Connessione a un sito Web per l'archiviazione di documenti e immagini.

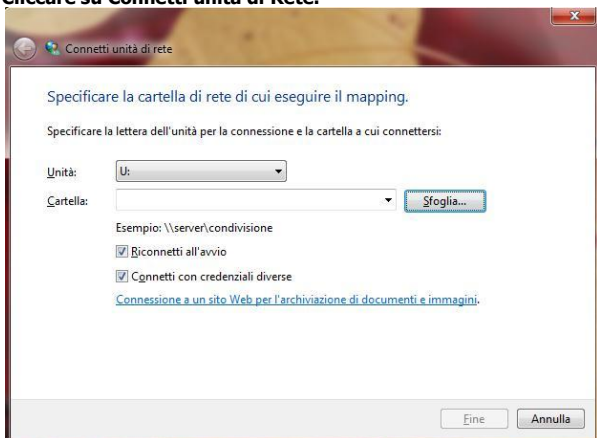
Fine Annulla

- Cliccare su **Sfoglia,** poi selezionare il nome precedentemente attribuito all'apparato **(NAS** nel caso di default) e poi la cartella **Storage** e cliccare su **OK.**
- Cliccare su **OK.** Non è richiesta alcuna password, salvo che non sia stato impostato il controllo d'accesso **(NAS->Access Control->Authorization Mode).**
- Spuntare la voce **Riconnetti all'avvio** e cliccare poi su **Fine.**

A questo punto è possibile accedere al disco inserito nel WebShare (utilizzando la cartella **Storage**) come fosse un disco del proprio PC.

	In caso di problemi è possibile forzare direttamente l'indirizzo IP dell'apparato per la mappatura di un'unità di rete usando la sintassi **\\192.168.1.254\Storage** nel campo **Cartella.** Cliccare su **OK.** Cliccare poi su **Fine.**

Creazione della Connessione Remota in Windows 7

In Windows 7 è possibile creare la connessione di Rete operando come segue:

- **Start->Computer**
- **Cliccare su Connetti unità di Rete.**

- Cliccare su **Sfoglia,** poi selezionare il nome precedentemente attribuito all'apparato **(NAS** nel caso di default) e poi la cartella **Storage** e cliccare su **OK.**
- Spuntare la voce **Riconnetti all'avvio.** Cliccare su **Fine.**

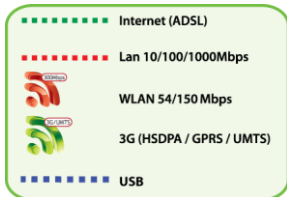
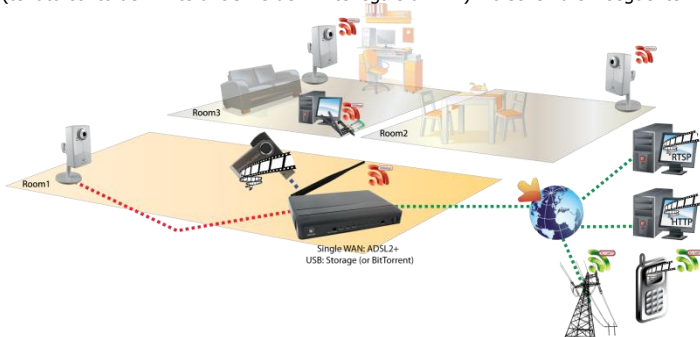
A questo punto è possibile accedere al disco inserito nel WebShare (utilizzando la cartella **Storage**) come fosse un disco del proprio PC.

In caso di problemi è possibile forzare direttamente l'indirizzo IP dell'apparato per la mappatura di un'unità di rete usando la sintassi **\\192.168.1.254\Storage** nel campo **Cartella.** Cliccare su **OK.** Cliccare poi su **Fine.**

APPENDICE I: FUNZIONE NVR su A02-RAU242-WN

Tramite questa funzionalità, disponibile su tutti i prodotti della famiglia NetCamera (dal firmware 1.16.17.01) e Mycam, è possibile inviare ad un qualunque NAS direttamente i filmati ripresi dal dispositivo in maniera continuativa o su motion detection (sino a 3 zone liberamente configurabili).
Si Voglia ad esempio direttamente salvare su una chiavetta da 8GB collegata al **A02-RAU242-WN(**con IP di default 192.168.1.254**)** quanto più tempo possibile (tenuto conto del limite di 8GB e del limite legale di 24H). Lo schema è il seguente:

Room3
Room2
Room1
RTSP
HTTP
Single WAN: ADSL2+
USB: Storage (or BitTorrent)

Internet (ADSL)
Lan 10/100/1000Mbps
WLAN 54/150 Mbps
3G (HSDPA / GPRS / UMTS)
USB

- Su A02-RAU242-WN: Accedere in **Advanced->NAS->Disk Utility** e cliccare su **Format.**
- Su A02-RAU242-WN: Accedere in **Advanced->NAS->Access Control** e spuntare la voce **Authorization Mode.** Cliccare **User Configuration,** digitare **Username** e **Password** e poi **Add.**
- Su A02-IPCAM8: **Setting->Events->Network Storage->General** ed utilizzare i seguenti settaggi, e cliccare poi su **Test** per verificare che tutto sia corretto ed infine su **OK.**

Parametro	Descrizione
Network Storage	**ON**
Protocol	**SMB/CIFS**
Network Storage Location	**\\192.168.1.254\Storage**
WorkGroup	
Username	Digitare la **User name** impostata nel **WebShare 242 WN**
Password	Digitare la **Password** impostata nel **WebShare 242 WN**
Re-Type Password	Digitare nuovamente la **Password** impostata nel **WebShare 242 WN**
OK	Cliccare per salvare i settaggi e tornare alla pagina di configurazione principale.
Cancel	Cliccare per tornare ai valori preimpostati nella maschera.
Test	Cliccare per verificare che le impostazioni siano corrette (**#Network storage test OK**).

- Su A02-IPCAM8: **Setting->Events->Network Storage->Periodical Recording** ed utilizzare i seguenti settaggi. Cliccare poi su **OK.**

Parametro	Descrizione
Periodical Recording	**ON**
Image File Name	**A02-IPCAM8**
Suffix	**Date Time**
File Size	**3**
Cyclic Size	4000*
Password	Digitare la password dell'account creato sul NAS.
Recording Time	**Always**

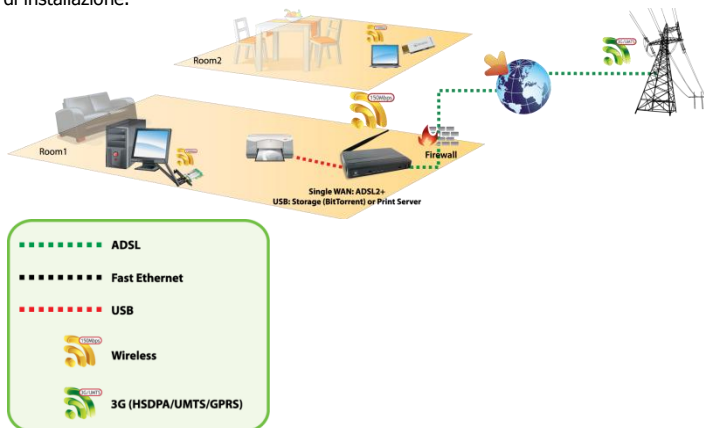
- Su A02-IPCAM8: **Setting->Mpeg4->Computer View->Quality=Fixed BitRate=512Kb.**

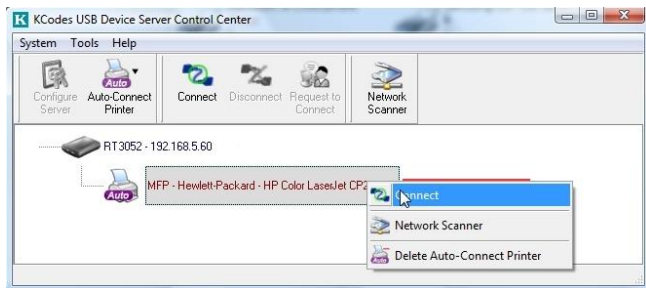
	Nell'esempio in questione, ogni file da 3MB è lungo all'incirca 55s. Pertanto 55S*(4000MB/3MB)=173333s di registrazione. Questa valore è inferiore a quello massimo conservabile pari ad

	86400s (24h). Date le condizioni, il valore massimo impostabile è **4712MB (**ottenuto come 3MB*86400S/55s)

	Tale valore deve essere ovviamente inferiore allo spazio disponibile sulla periferica di memorizzazione. Si raccomanda di non allocare più dell'85% dello spazio disponibile.

APPENDICE L: FUNZIONE Print Server

Tramite questa funzionalità è possibile connettere alla porta USB del WebShare una stampante e renderla a tuuti gli effetti una stampante di rete. In figura un esempio di installazione.

E' opportuno innanzitutto installare il software KCodes USB Devices Server.

- Verificare che la stampante sia inclusa nella lista di compatibilità.
- Procedere all'installazione della stampante sul proprio PC e verificare che questa stampi correttamente.
- Installare, per i soli ambienti Windows Vista/7, il software contenuto nella cartella **CDRom:\\A02-RAU242-WN\Utility\Setup.exe** del CDRom fornito a corredo.
- Lanciare **KCodes USB Devices Server.**

- Verrà evidenziato l'indirizzo **IP** utilizzato dal WebShare 242WN (ed il chipset in uso sul dispositivo: RT3050/52) e la stampante collegata. Selezionare la stampante e cliccare il tatso destro del mouse. Selezionare poi **Connect.** Il sistema provvederà ad effettuare l'installazione dei driver.

	La stampante può essere connessa ed usata da un utente per volta. Se questa è già connessa ad un altro utente non risulta disponibile (verrà inviata una richiesta di disconnessione all'utente proprietario, cjhe se accettata permetterà la nuova connessione).

	Selezionare **Auto-Connect Printer** per connettere la stampante automaticamente al PC.
	Accedendo al menu **Tools->Configuration** è possbile scegliere la lingua di visualizzazione e forzare l'autostartup dell'utility ad ogni avvio di windows.

APPENDICE M: Caratteristiche Tecniche

A02-RAU242-WN	
WAN Interface	(ADSL2+): RJ11
LAN Interface	4 x RJ45 10/100 Base-T Ethernet ports (auto MDI/MDI-X)
USB Interface	USB 2.0
WIRELESS Interface	1 X 5 dBi external orientable R-SMA Antenna
LED	7 diagnostic LEDs
Button	Reset, WPS and Power/WLAN Switch
Chipset	Ralink® 3050/52 (Wireless) TrendChip® TC3162LE (ADSL2+)
ADSL	• Full Rate ANSI T1.413 issue 2 • ITU G.992.1 (G.dmt), ITU G.992.2 (G.lite), ITU G.994.1 (G.hs)
ADSL2	• ITU G.992.3 (G.dmt.bis) [12Mbps download, 1 Mbps upload] • ITU G.992.3 Annex M
ADSL2+	• ITU G.992.5 (G.dmt.bisplus) [24Mbps download, 1 Mbps upload] • ITU G.992.5 Annex M
ATM	ATM Adaptation Layer Type 5(AAL5) and ATM service class: CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0
Wireless	• Standard IEEE802.11g/n and IEEE802.11b • DSSS (Direct Sequence Spread Spectrum) • Modulation: QPSK / BPSK / CCK and OFDM • RF Frequency: 2.400 GHz ~2.472GHz • Media Access Protocol: CSMA/CA with ACK • Operating Channel: 13 (Europe) • Data Rate (with automatic adaptation): 802.11n (Up to 150Mbps) with Automatic Fall-Back • Transmitting Power: 802.11g/n: up to 14 ± 0.5 dBm • Coverage Area: [Outdoor <120m / Indoor <35m] • 1 X 5 dBi external RSMA Antenna

	• Wi-Fi Protected Access (WPA-PSK, WPA2-PSK) and WEP 64/128 bit • WPS™
WDS	Up to 4 devices (WEP mode)
Receiver Sensitivity	• 802.11b (1Mbps): -90dBm @8% PER • 802.11b (6Mbps): -88dBm @8% PER • 802.11b (11Mbps): -85dBm @8% PER • 802.11g (54Mbps): -68dBm @10% PER • 802.11n (150Mbps): -68dBm @10% PER
Protocols	• RIP1, RIP2, STATIC ROUTING,IP, ICMP, TCP, UDP, IGMP • Payload encapsulation: RFC 2364 (PPPoA), RFC 2516 (PPPoE) and RFC 1483 Routed and Bridge
Management	• Easy Web GUI (also remote) • Firmware upgrade from local (Web, Telnet) • SNMP MIB support • Wizard Configuration Assistant (WEB)
Firewall and Security	• NAT, PAP, CHAP • SOHO Firewall Security with NAT Technology and Packet Filtering (Scheduled) • URL and Domani • SPI, URL and Application Filter • Password protection for system management • VPN (IPSec, PPTP) pass through
QoS	• The Quality of Service (QoS) ensures that VoIP and multimedia traffic are prioritized for improved quality
Advanced Features over USB Port	• 3G USB Modem (Dual Wan Configuration) • Samba Over USB • Print Server over USB Port • FTP Server embedded • iTunes embedded • BitTorrent client embedded
Support Internet Application	• Web, FTP, ICQ, Telnet, E-Mail, News, Netmeeting, MS messanger, PCanywhere, mIRC, CuSeeme...

Advanced Characteristics	• Wizard Setup • UPnP, Virtual Server (with PAT) and DMZ • Dynamic DNS • DNS, DNS relay and IGMP proxy • DHCP server (with Fixed Host), DHCP client, SNTP • Email Alert, SNMP V1.V2c, Wake on LAN, SysLog Server
Power Consumption:	9V ± 5%@ 1,5A
Certifications	CE (Europe)
Dimensions(mm)	155mm x 110mm x 24mm
Temperature Range	• Operation: 0°C ~ 32°C • Storage: -10°C ~ 60°C
Humidity	10% ~ 75% (non Condensing)
Weight	225g (without AC Adapter)
System Requirements (Router)	• TCP/IP protocol must be installed on each PC • Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
Package Contents	• WebShare Torrent 242 WN • RJ11 ADSL/telephone cable, CAT5 LAN cable and 5 dBi Antenna • Power Adapter (AC-DC, 9V@1,5A) • Quick Start Guide (English, French and Italian) • CD-Rom with Utility, Driver and Manual (English and Italian) • 1 x Warranty Card and 1 x WEEE Card

Specifications are subjected to change without prior notice. No liability for technical errors and/or omissions. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Users must comply with all applicable laws and regulations when using BitTorrent download service. Please check on the web site the compatibility list for supported Printers, 3G USB Modem and USB Storage. Please don't change TX Power Level into wireless setting.

 Le specifiche riportate possono cambiare senza preavviso. Nessuna responsabilità per errori e/o omissioni. Le condizioni ambientali e di utilizzo possono pesantemente influenzare il throughput atteso. L'utente deve rispettare le regolamentazioni vigenti quando utilizza il servizio BitTorrent integrato. Consultare preventivamente la lista di compatibilità sul sito per le stampanti /USB 3G Modem/periferiche di memorizzazione USB supportate dal dispositivo. Dispositivi non inclusi potrebbero non funzionare del tutto o generare errori imprevisti. I settaggi Wireless di default consentono un funzionamento ottimale del dispositivo, si invita a non cambiare il campo TX Power Level